DEU

7links™

3,5G UMTS Broadband Router und Access Point

PX-8569-675

INHALTSVERZEICHNIS

EINLEITUNG

Ihr neuer UMTS/EDGE-Router 5
Lieferumfang 5

Hinweise zur Nutzung dieser Bedienungsanleitung 6
Verwendete Symbole 6
Verwendete Textmittel 6
Gliederung 7

Sicherheitshinweise & Gewährleistung 8

Produktdetails 9
Router-Anschlüsse 9
Status-LEDs 9

Produktinformationen 10

Vorbereitung 11
Produktempfehlungen 12
Inbetriebnahme 12

INSTALLATIONS-ANLEITUNG FÜR EINSTEIGER

Die Installation 14
Den Computer vorbereiten 14
Der erste Zugriff auf den Router 15
Die Konfiguration als einzelner Router mit UMTS/EDGE-Verbindung 16
Einbindung des vorkonfigurierten Routers ins Netzwerk 18
Die Konfiguration als Zweitrouter 20

Sicherheitseinstellungen vornehmen 26
Einrichten der WPA/WPA2-Verschlüsselung 26
Verwenden der MAC-Filterfunktion Whitelist 28
Den Router mit einem Passwort sichern 30

Abschließende Worte 31

DETAILLIERTE ERLÄUTERUNGEN ZUR KONFIGURATION

Schnellkonfiguration 33

Schnellreferenz der Konfigurations-einstellungen mit Beispielen 34

7links™

ANHANG

Basiswissen Netzwerke 71
Hardware 71
Grundlegende Netzwerkbegriffe 73
Dienste in Netzwerken 77

Sicherheitsmaßnahmen in WLAN-Netzwerken 80

Informationen zur Entsorgung von elektronischen Geräten 81

Technische Daten 82

Konformitätserklärung 83

Checkliste für die Konfiguration 84

EINLEITUNG

IHR NEUER UMTS/EDGE-ROUTER

Sehr geehrte Kunden,

vielen Dank für den Kauf dieses UMTS/EDGE-Routers. Mit dieser innovativen Lösung aus dem Hause 7Links haben Sie nun auch als Privatanwender die Möglichkeit Ihr WLAN-Netz über UMTS/EDGE mit dem Internet zu verbinden. Dabei müssen Sie keine Rücksicht mehr auf DSL- oder Breitbandkabel-Versorgung nehmen.
Aber auch im professionellen Bereich können Sie mit diesem Router teure Verkabelungsmaßnahmen vermeiden und Bereiche, die sonst nicht ans Firmennetz angeschlossen werden könnten, mit einem Netzzugang versorgen.
Bitte lesen Sie die Bedienungsanleitung und befolgen Sie die Hinweise und Tipps, damit Sie diesen WLAN-Router optimal nutzen können.

Lieferumfang

- WLAN-Router
- Software-CD (mit Bedienungsanleitung)
- Schnellstartanleitung

HINWEISE ZUR NUTZUNG DIESER BEDIENUNGSANLEITUNG

Um diese Bedienungsanleitung möglichst effektiv nutzen zu können, ist es notwendig, vorab einige Begriffe und Symbole zu erläutern, die Ihnen im Verlauf dieser Anleitung begegnen werden.

Verwendete Symbole

	Dieses Symbol steht für mögliche Gefahren und wichtige Informationen im Umgang mit diesem Produkt. Es wird immer dann verwendet, wenn der Anwender eindringlich auf etwas hingewiesen werden soll.
	Dieses Symbol steht für nützliche Hinweise und Informationen, die im Umgang mit dem Produkt helfen sollen „Klippen zu umschiffen“ und „Hürden zu nehmen“.
	Dieses Symbol wird für beispielhafte Anwendungen und Erläuterungen verwendet, die oft komplexe Vorgehensweisen veranschaulichen und begreiflich machen sollen.
	Dieses Symbol wird oftmals hinter Fachbegriffen zu finden sein, zu denen weitere Erläuterungen im Glossar zu finden sind. Das Glossar soll dabei helfen, diese Fachbegriffe für den Laien verständlich zu machen und in einen Zusammenhang zu rücken.

Verwendete Textmittel

GROSSBUCHSTABEN	Großbuchstaben werden immer dann verwendet, wenn es gilt Tasten, Anschluss- oder andere Produkt-Beschriftungen kenntlich zu machen.
Fettschrift	Fettschrift wird immer dann eingesetzt, wenn Menüpunkte oder genau so bezeichnete Ausdrücke in der Software des Produktes verwendet werden.
1. Aufzählungen 2. Aufzählungen 3. Aufzählungen	Aufzählungen werden immer dann verwendet, wenn der Anwender eine bestimmte Reihenfolge von Schritten befolgen soll, oder die Merkmale des Produktes beziffert werden sollen.
<Platzhalter>	Im zweiten Teil des Handbuches werden Platzhalter verwendet. Diese Platzhalter werden in < und > Zeichen eingegrenzt. <text> bedeutet hierbei die Möglichkeit freie Eingaben zu machen (oftmals IP-Adressen ◪). <parameter> bedeutet die Möglichkeit mehrere benötigte Daten einzugeben. <datei> wird verwendet, wenn ein Dateiname erforderlich ist. <hexcode> bezeichnet eine Eingabe in Hexadezimalen Ziffern.

Gliederung

Diese Anleitung ist untergliedert in vier grundlegende Bestandteile:

Einleitung	Erläuterungen zur Nutzung dieser Anleitung, Wichtige Hinweise zur Sicherheit im Umgang mit dem Produkt, Übersicht über das Produkt
Installationsanleitung für Einsteiger	Detaillierte Anleitung zur Installation und Inbetriebnahme des Routers in einem bestehenden WLAN-Netzwerk, oder als allein stehender Router. Anleitung zur Konfiguration von grundlegenden Sicherheitsmaßnahmen.
Detaillierte Erläuterungen zur Konfiguration	Dieser Teil der Anleitung richtet sich insbesondere an fortgeschrittene Anwender und Profis. Hier finden sich genaue Informationen zu den einzelnen Konfigurations-möglichkeiten und Anwendungsbeispiele für den Einsatz des Routers in größeren Netzwerken und Betrieben.
Anhang	Troubleshooting (Problemlösungen), Glossar, Technische Daten, Konformitätserklärung, Index

SICHERHEITSHINWEISE & GEWÄHRLEISTUNG

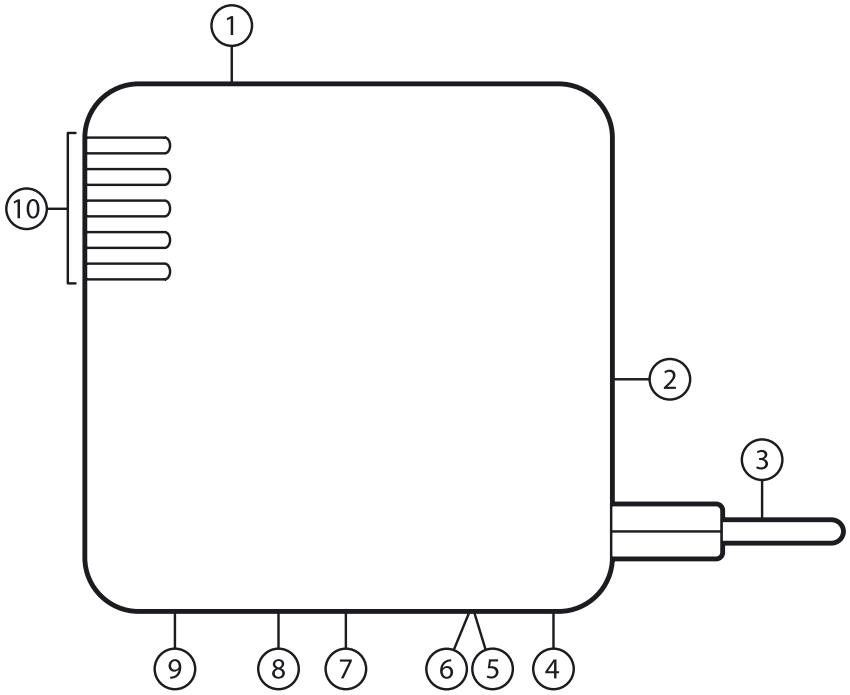
- Diese Bedienungsanleitung dient dazu, Sie mit der Funktionsweise dieses Produktes vertraut zu machen. Bewahren Sie diese Anleitung daher stets gut auf, damit Sie jederzeit darauf zugreifen können.
- Sie erhalten bei Kauf dieses Produktes zwei Jahre Gewährleistung auf Defekt bei sachgemäßem Gebrauch. Bitte beachten Sie auch die allgemeinen Geschäftsbedingungen!
- Bitte verwenden Sie das Produkt nur in seiner bestimmungsgemäßen Art und Weise. Eine anderweitige Verwendung führt eventuell zu Beschädigungen am Produkt oder in der Umgebung des Produktes.
- Ein Umbauen oder Verändern des Produktes beeinträchtigt die Produktsicherheit. Achtung Verletzungsgefahr!
- Führen Sie Reparaturen nie selber aus!
- Behandeln Sie das Produkt sorgfältig. Es kann durch Stöße, Schläge oder Fall aus bereits geringer Höhe beschädigt werden.
- Halten Sie das Produkt fern von Feuchtigkeit und extremer Hitze.
- Tauchen Sie das Produkt niemals in Wasser oder andere Flüssigkeiten.
- Schließen Sie das Produkt nicht an extrem gespannte Kabel an. Die Anschlüsse können sonst beschädigt werden.
- Verlegen Sie Kabel möglichst unzugänglich in Kabelkanälen, um Beschädigungen und „Stolperfallen“ zu vermeiden.
- Verwenden Sie Funkprodukte niemals in direkter Nähe von Personen mit elektronischen Herzschrittmachern!

ACHTUNG
Es wird keine Haftung für Folgeschäden übernommen.
Technische Änderungen und Irrtümer vorbehalten!

PRODUKTDETAILS

Router-Anschlüsse

1. USB-Stromversorgung
2. Modus-Schalter
3. Strom-Anschluss
4. Verriegelung für Stecker
5. WPS-Taste
6. Reset-Taste
7. LAN/WAN-Port
8. LAN-Port
9. USB-Ports
10. Status-LEDs



Status-LEDs (10)

1. WAN-LED: zeigt den Status der Hauptverbindung an.
2. LAN-LEDs: zeigen den Status der Nebenverbindungen an.
3. Wireless-LED: zeigt den Status des WLANs an.
4. POWER-LED: zeigt den Betriebszustand an.
5. STATUS-LED: zeigt die Betriebsbereitschaft an.

PRODUKTINFORMATIONEN

Der WLAN-Router wurde speziell für den Office-Bereich entwickelt und bietet neben reinen Routingaufgaben auch die Möglichkeit als Bridge oder WLAN-Repeater zu fungieren.
Dadurch lässt sich dieses Produkt äußerst vielseitig einsetzen und bietet sowohl dem Heimanwender, als auch professionellen Nutzern eine Vielzahl an Anwendungsgebieten.
Die integrierte UMTS/EDGE-Stick-Unterstützung bietet auch in Gebieten, die nicht mit DSL oder schnellen Kabelanschlüssen versorgt sind, eine optimale Anbindungsmöglichkeit.
Komplettiert werden die Standard-Funktionen des Routers durch die Unterstützung von Samba-Netzwerken (Windows Dateifreigabe), USB-Druckern (als Printserver) sowie einem FTP-Server für angeschlossene USB-Festplatten.
Damit lassen sich sowohl private Netzwerke als auch Netzwerke kleinerer und mittlerer Betriebe optimal aufbauen und erweitern.
Hierzu stehen ebenfalls die zum heutigen Sicherheitsstandard gehörenden Verschlüsselungsvarianten WPA und WPA2 zur Verfügung – und auch RADIUS-Server werden unterstützt.
Mit den 802.11b/g/n Standards erreichen Sie Datendurchsatzraten bis zu 600 MBit/s. Die integrierte Antenne bietet Ihnen unter Arbeitsbedingungen etwa eine Reichweite bis zu 30 Meter in Gebäuden (abhängig von der Bausubstanz).

VORBEREITUNG

HINWEIS:
Viele der Fachbegriffe werden im Anhang der Bedienungsanleitung unter „Basiswissen Netzwerke“ erläutert. Sollten dennoch Fragen bezüglich der Installation bestehen, können Sie sich gerne an unsere Service-Hotline wenden.

HINWEIS:
Sollten Sie sich bei den folgenden Fragen nicht sicher sein, empfehlen wir Ihnen sich an einen Fachmann zu wenden. Eine Fehlkonfiguration des Routers kann unter bestimmten Umständen Ihr Netzwerk beträchtlich in der Funktion stören.

Um eine reibungslose Installation des Routers gewährleisten zu können, sollten Sie folgende Daten im Vorfeld recherchieren und bereithalten:

1. Die Zugangsdaten Ihres Serviceproviders (Internet-Anbieters)
2. Die IP-Adresse des Gateway-Routers, sofern Sie den WLAN-Router nicht als einzigen Router im Netzwerk betreiben wollen.
3. Wird in Ihrem Netzwerk bereits ein DHCP-Server verwendet? Wenn ja – welche Adressräume deckt dieser ab?
4. Welche Protokolle werden für verschiedene Anwendungen verwendet und benötigt (etwa uPnP)?
5. Welche Daten hat Ihnen der Mobilfunkanbieter zusammen mit dem UMTS-Stick überlassen?

Ferner sollten Sie folgendes im Vorfeld beachten:

- Bei der Erstinstallation sollte der Router direkt über Kabel mit einem Computer verbunden werden.
- Beseitigen Sie eventuelle Störquellen im Funktionsbereich des WLAN-Routers. Hierzu gehören Funktelefone, Funküberwachungskameras und andere Geräte, die mit dem 2,4 GHz Band funktionieren.
- Sichern Sie die Stromversorgung möglichst mit einem Überspannungsschutz.
- Verwenden Sie zwischen Netzwerkgeräten und Router kein Kabel, das länger als 25 m ist – bei ungünstigen Verhältnissen kann es sonst zu einem Spannungsabfall kommen und der Router kann die übertragenen Daten nicht mehr korrekt empfangen.
- Schalten Sie zur Einbindung des Routers in ein bestehendes Netzwerk alle Firewalls, Virenscanner, MAC-Adressenfilter und Verschlüsselungen bei Ihrem bereits vorhandenen Router aus.
- Notieren Sie sich die SSID Ihres bestehenden WLAN-Netzwerks.

HINWEIS:
Im Anhang (S.86) finden Sie eine Checkliste, die Ihnen als Stütze dienen soll und in die Sie die entsprechenden Werte eintragen können. Drucken Sie die Checkliste einfach aus.

Produktempfehlungen
Zusätzlich zu den unbedingt notwendigen Zubehörteilen empfehlen wir Ihnen für die Erweiterung Ihres Netzwerkes folgende Artikel aus dem Sortiment unter www.pearl.de:

PE-8419-675	Netzwerkkabel Twisted Pair 2 x RJ45 Stecker-Stecker 20m
PE-219-675	Netzwerkkabel Twisted Pair 2 x RJ45 Stecker-Stecker 10m
PE-218-675	Netzwerkkabel Twisted Pair 2 x RJ45 Stecker-Stecker 5m
PE-217-675	Netzwerkkabel Twisted Pair 2 x RJ45 Stecker-Stecker 3m
PE-5586-675	ConnecTec 10/100MBit Netzwerk-Switch 5-Port USB mit blauen LEDs
PX-6516-675	TP-LINK 54Mbit WLAN-USB-Dongle „TL-WN321G“ USB2.0 (802.11g/b)
PE-4454-675	revolt Profi-Steckdosenleiste mit Netzwerkschutz

Inbetriebnahme

HINWEIS:
Beim Verlegen der Kabel sollten Sie darauf achten, die Kabel nicht einzuklemmen oder anderweitig zu beschädigen. Ziehen Sie gegebenenfalls einen Fachmann hinzu.

Schieben Sie den Steckdosen-Adapter in die entsprechende Führung am Router. Drücken Sie hierzu nötigenfalls die Verriegelung nach links.
Stecken Sie anschließend den Router in eine möglichst gesicherte (Überspannungsschutz) Steckdose in Anschlussreichweite des Computers, über den Sie den Router konfigurieren wollen.

INSTALLATIONS-ANLEITUNG FÜR EINSTEIGER

DIE INSTALLATION

Den Computer vorbereiten
Im Auslieferungszustand ist der DHCP-Server des Routers aktiviert. Daher sollte der Konfigurationscomputer ebenfalls auf DHCP-Zuweisung umgestellt werden, sofern dies nicht bereits der Fall ist.

- **Vorgehensweise unter Windows 2000 und Windows XP**
  1. Klicken Sie auf den Start-Button.
  2. Klicken Sie auf **Systemsteuerung**.
  3. Wählen Sie **Netzwerkverbindungen**.
  4. Doppelklicken Sie die aktive LAN-Verbindung (unter **Status** steht **Verbindung hergestellt**).
  5. Klicken Sie auf **Eigenschaften**.
  6. Markieren Sie im Auswahlfenster **Internetprotokoll (TCP/IP)** und klicken Sie auf **Eigenschaften**.
  7. Wählen Sie **IP-Adresse automatisch beziehen** und **DNS-Serveradresse automatisch beziehen** aus und bestätigen Sie mit **OK**, um die Änderungen zu speichern.

- **Vorgehensweise unter Windows Vista und Windows 7**
  1. Klicken Sie auf den Start-Button.
  2. Klicken Sie auf **Systemsteuerung**.
  3. Wählen Sie **Netzwerk- und Freigabecenter**.
  4. Klicken Sie die hinter der aktiven LAN-Verbindung auf **Status anzeigen**.
  5. Klicken Sie auf **Eigenschaften**.
  6. Markieren Sie im Auswahlfenster **Internetprotokoll Version 4 (TCP/IPv4)** und klicken Sie auf **Eigenschaften**.
  7. Wählen Sie **IP-Adresse automatisch beziehen** und **DNS-Serveradresse automatisch beziehen** aus und bestätigen Sie mit **OK**, um die Änderungen zu speichern.

Der erste Zugriff auf den Router

HINWEIS:
Um die Konfigurationsseite des Routers korrekt darzustellen, muss in Ihrem Browser die Darstellung von JavaScript erlaubt sein. Ziehen Sie gegebenenfalls die Hilfefunktion Ihres Browsers zu Rate.

Starten Sie auf dem Computer einen Browser (wie etwa den **Internet Explorer**, **Firefox**, oder ähnliche).

HINWEIS:
Wenn die Konfigurationsseite nicht korrekt dargestellt wird oder nicht korrekt funktioniert, verwenden Sie einen anderen Browser.

Geben Sie in der Adresszeile des Browsers die IP-Adresse des Routers ein, um zum Konfigurationsbildschirm zu gelangen. Bei der ersten Installation ist die IP-Adresse des Routers **192.168.1.1**. Diese Adresse können Sie im Verlauf der Erstinstallation ändern. Nachdem Sie die Adresse eingegeben haben, zeigt Ihr Browser die Einsprungseite des Routers an.

Klicken Sie hier auf den Button **Administrator**.
Im anschließenden Anmeldebildschirm geben Sie in den Feldern **Benutzername** und **Passwort** jeweils **admin** ein. Dies sind die Standard-Anmeldedaten und werden auch nach dem Zurücksetzen auf die Werkseinstellungen wiederhergestellt.

Die Konfiguration als einzelner Router mit UMTS/EDGE-Verbindung

ACHTUNG:
In diesem Kapitel wird davon ausgegangen, dass Sie den Router als alleinigen Router verwenden und direkt eine Verbindung zum Internet mit diesem Router herstellen. Sollten Sie den Router jedoch als zweiten Router im Netzwerk verwenden, lesen Sie bitte im Kapitel* Die Konfiguration als Zweitrouter *in der Bedienungsanleitung weiter.

- **Vorkonfiguration des Routers**
  Um den Router für den Einsatz in Ihrem Netzwerk vorzubereiten, verwenden Sie den **Sofortsetup**-Assistenten. Dieser Assistent erlaubt eine schnelle und unkomplizierte Einbindung des Routers. Klicken Sie im Menü auf der linken Seite einfach auf **Sofortsetup**, um den Assistenten zu starten.

Wählen Sie zuerst eine Zeitzone, mit der die Systemzeit synchronisiert werden kann.

Der Punkt **Passwort ändern** sollte erst einmal nicht beachtet werden. Dies ist erst nach der Fertigstellung der Erstkonfiguration sinnvoll und sollte später unbedingt vorgenommen werden.

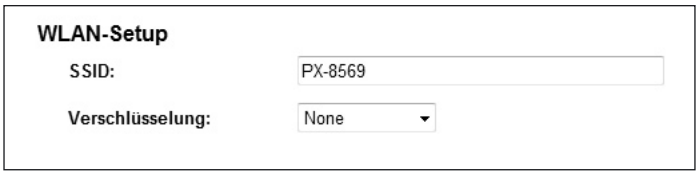
Gerätename kann ebenfalls so belassen werden. Dieser Wert ist für die Konfiguration als Router nicht relevant und wird nur für Windows-Netzwerkfreigaben benötigt.

Das **WAN Interface Setup** wird verwendet, um Ihren Router mit dem Internet zu verbinden. In dieser Bedienungsanleitung wird davon ausgegangen, dass Sie sich mit dem Internet über UMTS/EDGE verbinden.
Geben Sie hier unter **WAN-Schnittstelle** den Punkt **3.5G usb dongle** an.
Bei **Service** wählen Sie **UMTS/HSPA/HSDPA/HSUPA**.

ACHTUNG:
Sollte an Ihrem aktuellen Standort kein UMTS verfügbar sein, können Sie auch nacheinander die beiden anderen Auswahlmöglichkeiten versuchen. Warten Sie jeweils eine Weile, um dem Router die Möglichkeit zum Verbindungsaufbau zu geben (nach jeder Einstellung etwa 4-5 Minuten).

- **SIM-PIN** muss eingegeben werden, wenn die verwendete SIM-Karte durch einen PIN geschützt ist. Andernfalls aktivieren Sie den Haken bei **keine**.
- **SIM-PIN wiederholen** muss ausgefüllt werden, wenn Sie eine Angabe bei **SIM-PIN** gemacht haben.
- **APN** ist der Name des Zugriffspunktes Ihres Providers. Dieser wird auch häufig in den Unterlagen Ihres Mobilfunkbetreibers so genannt. Sollten Sie sich hier nicht sicher sein, kontaktieren Sie bitte den Mobilfunkbetreiber.
- **Benutzername** und **Kennwort** sind ebenfalls durch den Mobilfunkbetreiber festgelegt und können in dessen Unterlagen nachgelesen werden.
  Geben Sie diese Angaben ein und achten Sie dabei auf Groß- und Kleinschreibung.
- **Telefon** wird auch in den Zugangsdaten des Mobilfunkbetreibers angegeben. Die meisten Betreiber verwenden hier die Angabe: ***99***1#**.

Der Punkt **WLAN-Setup** wird benötigt, um den Router für den drahtlosen Zugriff zu konfigurieren. Geben Sie hier unter SSID den Namen an, den Ihr WLAN-Netzwerk verwenden soll.
Bei **Verschlüsselung** geben Sie vorerst **keine** an.

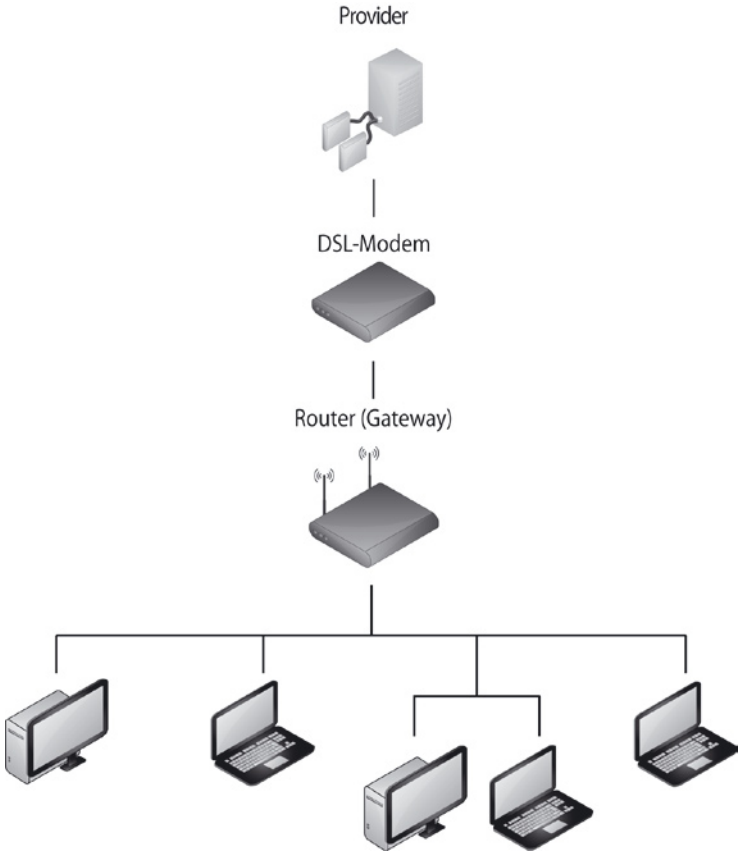


Die weiteren Punkte können bei der ersten Konfiguration ebenfalls außer Acht gelassen werden. Klicken Sie auf **Fertig stellen**, um die Konfiguration abzuschließen.

Einbindung des vorkonfigurierten Routers ins Netzwerk

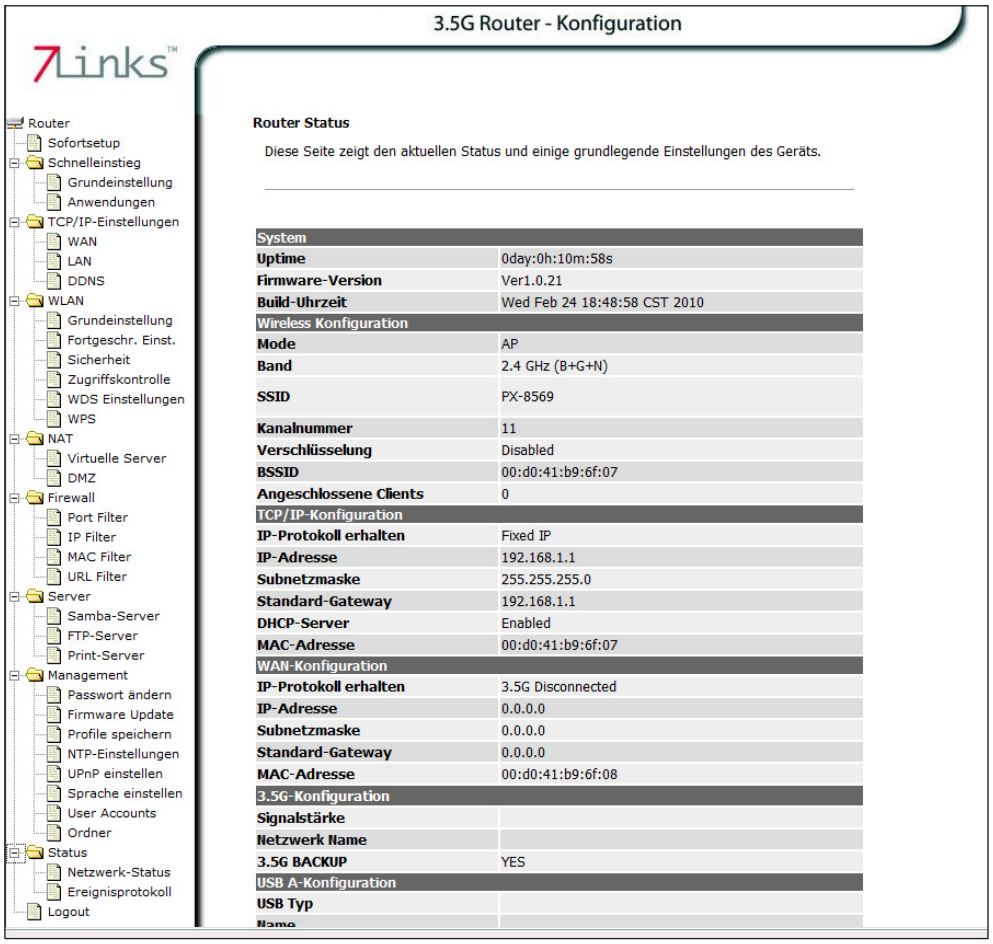
Nachdem Sie den Router vorbereitet haben, können Sie nun andere Netzwerkgeräte an den Router anschließen.

Wenn Sie mehrere Geräte per Kabel mit dem Router verbinden wollen, empfiehlt sich der Einsatz eines Netzwerk-Switches. Lesen Sie hierzu näheres im Glossar.



Zur Endkonfiguration sollte der Computer, von dem aus konfiguriert wird, per LAN-Kabel an das Netzwerk mit Ihrem neuen WLAN-Router angeschlossen sein. Später kann die Konfiguration kabellos erfolgen.

Geben Sie nun in Ihrem Browser die IP-Adresse des Routers ein (in diesem Fall die **192.168.1.1**).
Melden Sie sich wie bei der ersten Konfiguration als **admin** an.
Im Menübereich **Router** können Sie anschließend überprüfen, ob die Verbindung zu Ihrem Internetanbieter erfolgreich war. Die Daten über die Verbindung mit Ihrem Internetanbieter werden im Bereich **WAN** angezeigt.



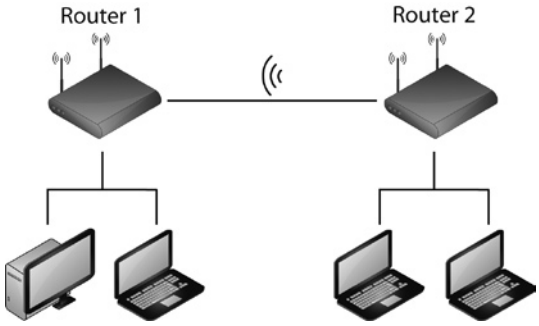
HINWEIS:
Nachdem Ihr Router in das bestehende Netzwerk eingebunden wurde, wird empfohlen im Menüpunkt **Sicherheit** *(Unterpunkt von* **WLAN***) eine sichere Verschlüsselungsmethode festzulegen! Lesen Sie hierzu das Kapitel „Sicherheits-einstellungen vornehmen“ auf S.26.*

Die Konfiguration als Zweitrouter

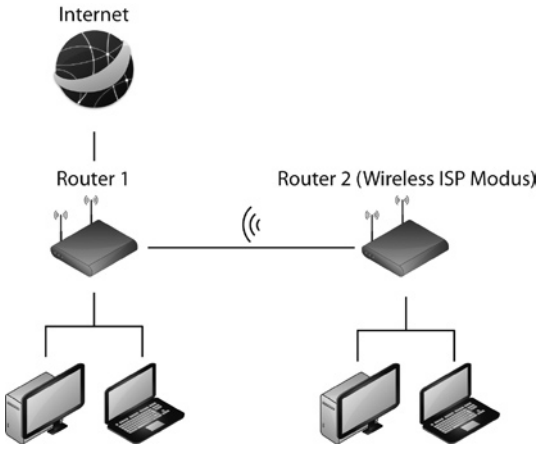
ACHTUNG:
In diesem Kapitel wird davon ausgegangen, dass Sie den Router als Zweitrouter im WLAN verwenden und nicht direkt eine Verbindung zum Internet mit diesem Router herstellen. Sollten Sie den Router jedoch als einzigen Router im Netzwerk verwenden, lesen Sie bitte im Kapitel Die Konfiguration als einzelner Router auf S.16 weiter.

- **Anwendungsmöglichkeiten**
  Um den Router für den Einsatz in Ihrem bestehenden Netzwerk vorzubereiten, sind nur wenige Handgriffe und Einstellungen notwendig. In den folgenden Schritten binden Sie Ihren neuen Router an den bereits vorhandenen Router als Bridge an. Dies bedeutet, dass Sie ein zweites, untergeordnetes Netzwerk aufbauen, mit dem Sie ebenfalls Zugriff auf das Internet haben. Diese Verwendung wird üblicherweise dann angestrebt, wenn die Reichweite eines WLANs vergrößert werden soll oder WLAN und verkabeltes LAN von zwei verschiedenen Stellen verwaltet werden sollen.

Bsp. 1

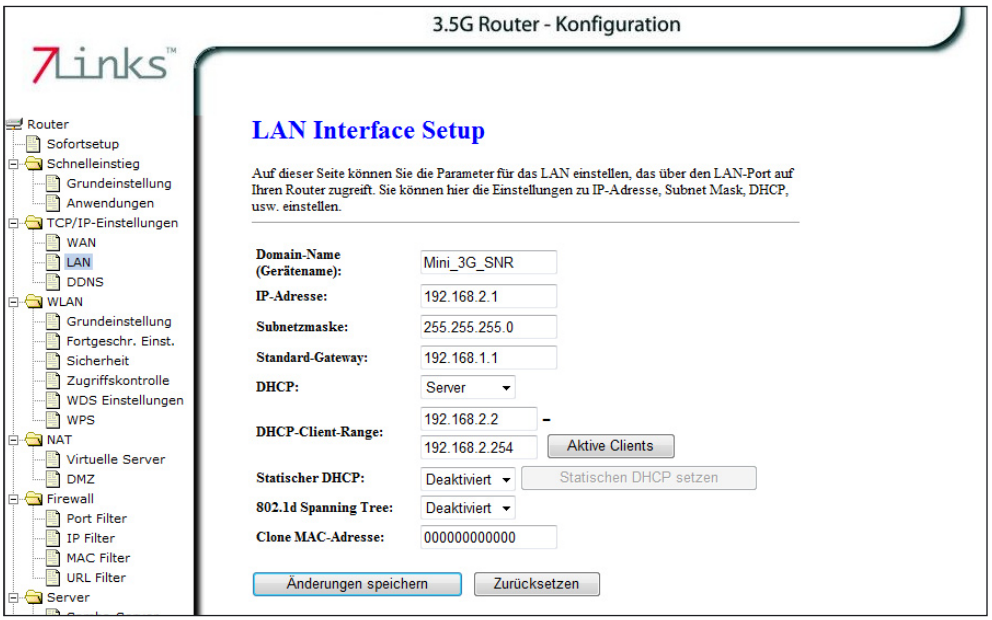


Bsp. 2



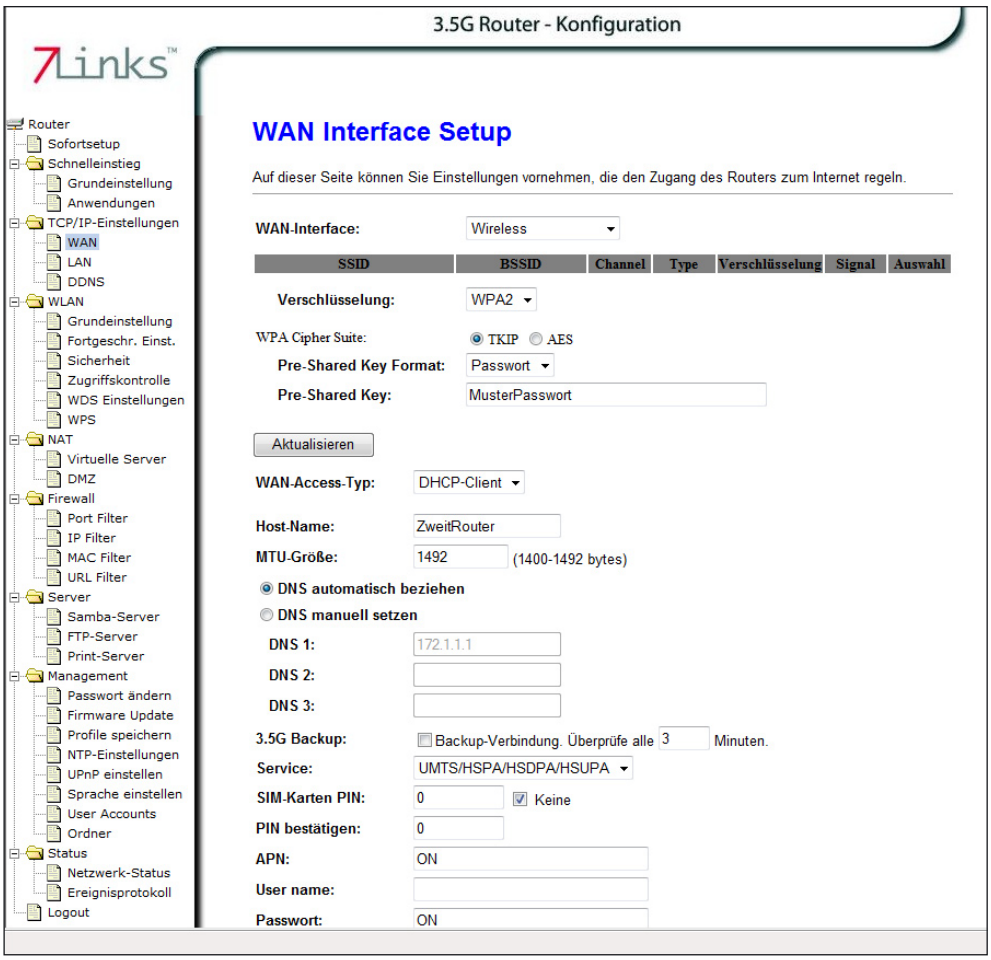
Im ersten Beispiel werden zwei WLAN-Router auf diese Weise miteinander verbunden. Das zweite Beispiel zeigt eine getrennte Verwaltung von LAN und WLAN mit gleichzeitiger Nutzung eines Internet-Anschlusses.

- **Ändern der Standard-IP-Adresse**
  Um ein zweites oder erweitertes Netzwerk verwenden zu können, muss zuerst der LAN-Zugang zum Router neu geregelt werden.
  Hierzu wird zuerst die LAN-Schnittstelle mit einer neuen IP-Adresse versehen:
  1. Wählen Sie in der Routerkonfiguration den Punkt **TCP/IP-Einstellungen** und dann **LAN**.
  2. Geben Sie bei **IP-Adresse** den Wert **192.168.2.1** ein, um ein neues Netzwerksegment zu verwenden.
  3. Die **Subnetzmaske** behält den Wert **255.255.255.0**.
  4. Als **Standard-Gateway** tragen Sie den Wert **192.168.1.1** ein.
  5. Wählen Sie bei **DHCP** die Option **Server**.
  6. Ändern Sie die **DHCP-Client-Range** auf **192.168.2.2** - **192.168.2.254**.
  7. Übernehmen Sie die Konfiguration mit **Änderungen speichern**.

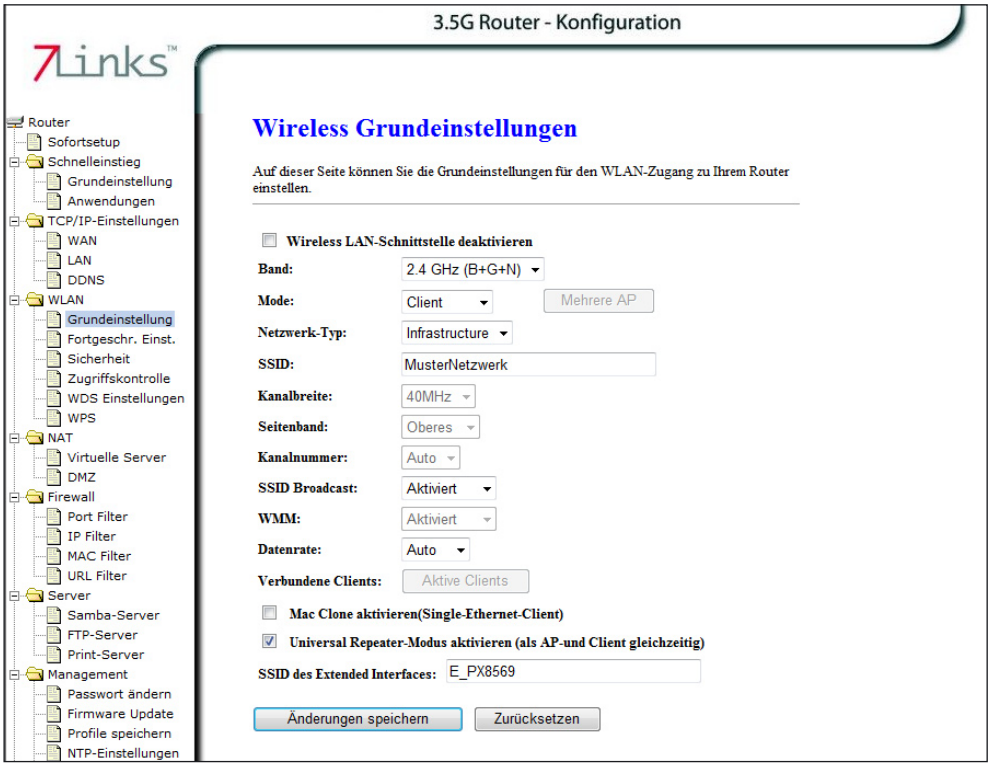


Konfiguration zu Beispiel 1

1. Wählen Sie in der Routerkonfiguration den Punkt **TCP/IP-Einstellungen** und dann **WAN**.
2. Stellen Sie **WAN-Interface** auf **Wireless**.
3. Klicken Sie auf **Aktualisieren**, um eine Liste der verfügbaren WLANs anzeigen zu lassen.
4. Wählen Sie in der Übersicht das WLAN aus, mit dem Sie sich verbinden wollen.
5. Wählen Sie bei **Verschlüsselung** die Verschlüsselungsvariante, die Ihr bestehendes WLAN-Netzwerk verwendet und geben Sie anschließend die benötigten Daten (Format, Passwort) ein.
6. Wählen Sie bei **WAN Access-Typ** den Punkt **DHCP-Client**.
7. Geben Sie dann bei **Host-Name** den Namen ein, der für den Router verwendet werden soll.
8. Die **MTU-Grösse** wird auf den Wert **1492** festgelegt.
9. Aktivieren Sie abschließend die Auswahl **DNS automatisch beziehen** und bestätigen Sie die Konfiguration mit Klick auf **Änderungen speichern**.



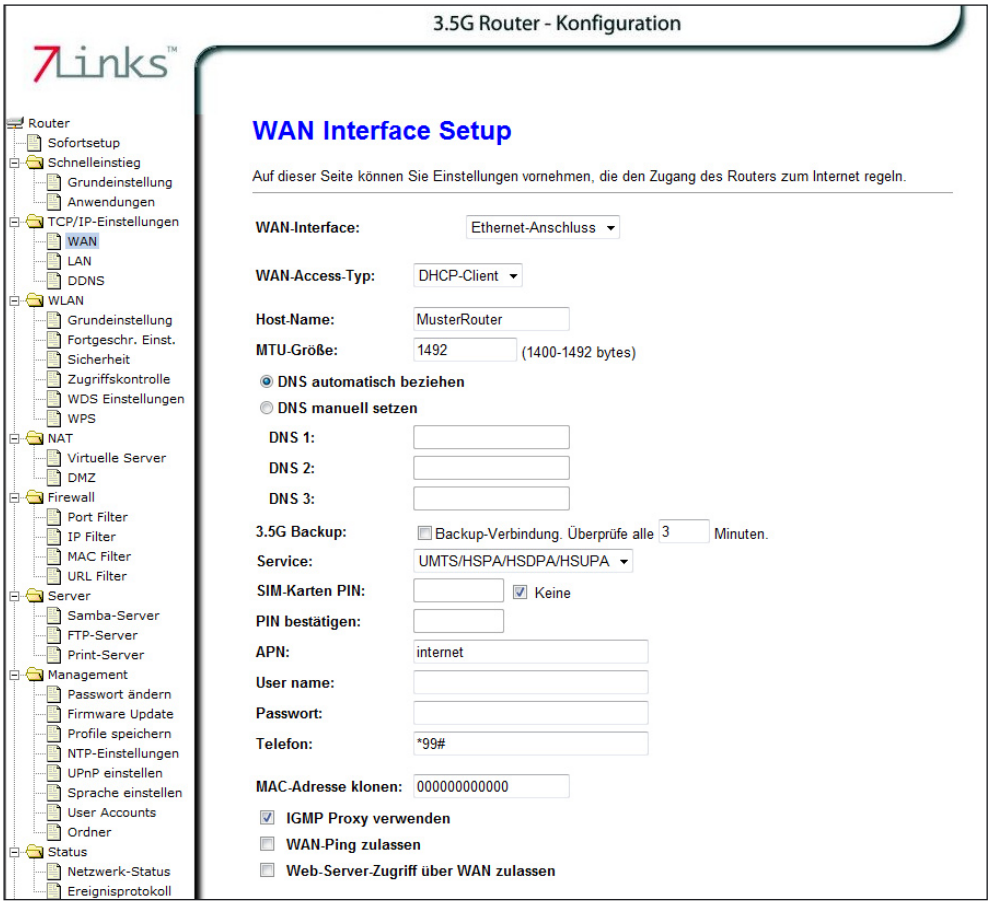
10. Wählen Sie in der Routerkonfiguration den Punkt **WLAN** und dann **Grundeinstellung**.
11. Wählen Sie als **Band 2.4 GHz (B+G+N)**.
12. Wählen Sie als Mode **Client**.
13. Geben Sie bei **SSID** die SSID Ihres bestehenden WLAN-Netzwerks ein.
14. Wählen Sie bei **Kanalnummer Auto**.
15. Aktivieren Sie den Haken bei **Universal-Repeater-Modus aktivieren**.
16. Geben Sie bei **SSID des Enhanced Interfaces** den Namen an, den Ihr erweitertes Netzwerk verwenden soll.
17. Klicken Sie auf **Änderungen speichern**.



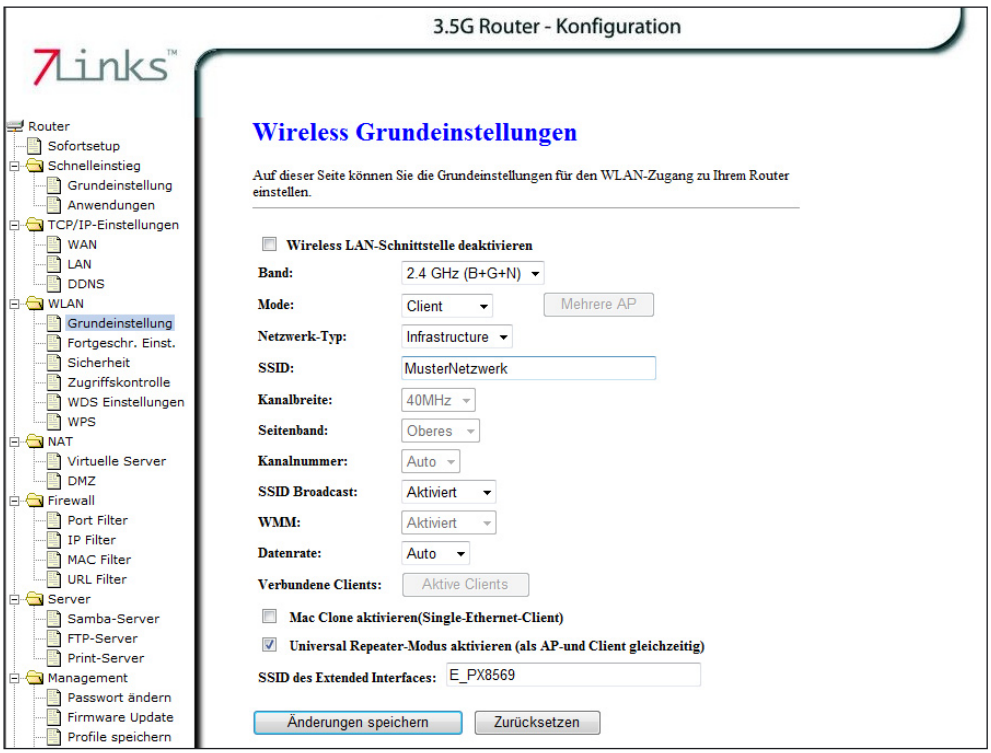
HINWEIS:
*Nachdem Ihr Router in das bestehende Netzwerk eingebunden wurde, wird empfohlen im Menüpunkt **Sicherheit** (Unterpunkt von **Wireless**) eine sichere Verschlüsselungsmethode festzulegen! Lesen Sie hierzu das Kapitel „Sicherheitseinstellungen vornehmen“ auf S.26.*

Konfiguration zu Beispiel 2

1. Wählen Sie in der Routerkonfiguration den Punkt **TCP/IP-Einstellungen** und dann **WAN**.
2. Stellen Sie **WAN-Interface** auf **Ethernet-Anschluss**.
3. Wählen Sie bei **WAN-Access-Typ** den Punkt **DHCP-Client**.
4. Geben Sie dann bei **Host-Name** den Namen ein, der für den Router verwendet werden soll.
5. Die **MTU-Größe** wird auf den Wert **1492** festgelegt.
6. Aktivieren Sie abschließend die Auswahl **DNS automatisch beziehen** und bestätigen Sie die Konfiguration mit Klick auf **Änderungen speichern**.



7. Wählen Sie in der Routerkonfiguration den Punkt **WLAN** und dann **Grundeinstellung**.
8. Wählen Sie als **Band 2.4 GHz (B+G+N)**.
9. Wählen Sie als Mode **Client**.
10. Geben Sie bei **SSID** die SSID Ihres bestehenden WLAN-Netzwerks ein.
11. Wählen Sie bei **Kanalnummer Auto**.
12. Aktivieren Sie den Haken bei **Universal Repeater-Modus aktivieren**.
13. Geben Sie bei **SSID des Enhanced Interfaces** den Namen an, den Ihr erweitertes Netzwerk verwenden soll.
14. Klicken Sie auf **Änderungen speichern**.



HINWEIS:
*Nachdem Ihr Router in das bestehende Netzwerk eingebunden wurde, wird empfohlen im Menüpunkt **Sicherheit** (Unterpunkt von **WLAN**) eine sichere Verschlüsselungsmethode festzulegen! Lesen Sie hierzu das nächste Kapitel.*

SICHERHEITSEINSTELLUNGEN VORNEHMEN

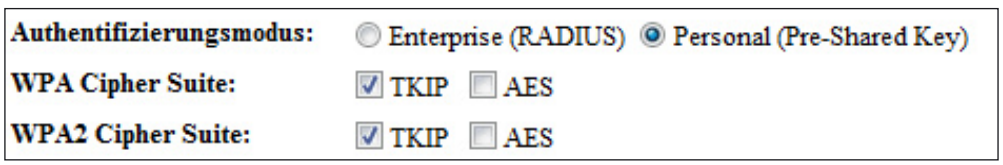
Um den unberechtigten Zugriff auf Ihr Netzwerk zu verhindern, ist es notwendig, entsprechende Sicherheitsmaßnahmen zu ergreifen. Fremde Nutzer könnten sonst ungehindert auf Ihre Computer zugreifen, die sich im Netzwerk befinden.
Der sicherste Weg, Ihr WLAN-Netzwerk zu schützen, ist die Verwendung der WPA2-Verschlüsselung und die Zugangsbeschränkung nur für erlaubte MAC-Adressen. Jedes Ihrer WLAN-Geräte besitzt eine einzigartige MAC-Adresse – vergleichbar mit einem Fingerabdruck.

HINWEIS:
Bevor Sie beginnen, einzelne Geräte endgültig in Ihr WLAN-Netzwerk einzubinden, müssen zuerst die entsprechenden Sicherheitseinstellungen am Router vorgenommen werden.

Einrichten der WPA/WPA2-Verschlüsselung
Rufen Sie in Ihrem Browser die Konfigurationseinstellungen Ihres Routers auf. Klicken Sie im Hauptmenü auf den Punkt **WLAN** und dann auf **Sicherheit**.

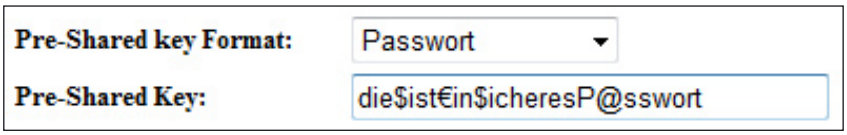
Wählen Sie als Verschlüsselung **WPA Mixed**. Damit stellen Sie sicher, dass auch ältere Geräte, die nur WPA-Verschlüsselung unterstützen ebenfalls mit Ihrem Netzwerk verbunden werden können.

Als nächstes nehmen Sie die Einstellungen zur WPA/WPA2-Verschlüsselung vor. Wählen Sie als Authentifizierungsmethode **Personal** und als **WPA/WPA2-Cipher-Suite** jeweils **TKIP**. Die Option **AES** sollten Sie nicht verwenden, da dies derzeit noch häufig zu Problemen beim Verbindungsaufbau zwischen zwei Geräten führt.



Nun wird noch ein Passwort für die Verbindung der Geräte benötigt. Stellen Sie hierzu bei **Pre-Shared Key Format** den Wert **Passwort** ein.
Im Feld **Pre-Shared Key** geben Sie anschließend das Passwort ein, mit dem Sie den Zugang zu Ihrem Netzwerk sicher wollen.

HINWEIS:
Ein Passwort sollte möglichst aus mehr als 6 Zeichen und einigen Sonderzeichen (z.B. @, $, ?, !, usw.) bestehen. Notieren Sie sich das Passwort nötigenfalls und geben Sie dieses nicht an Außenstehende weiter.

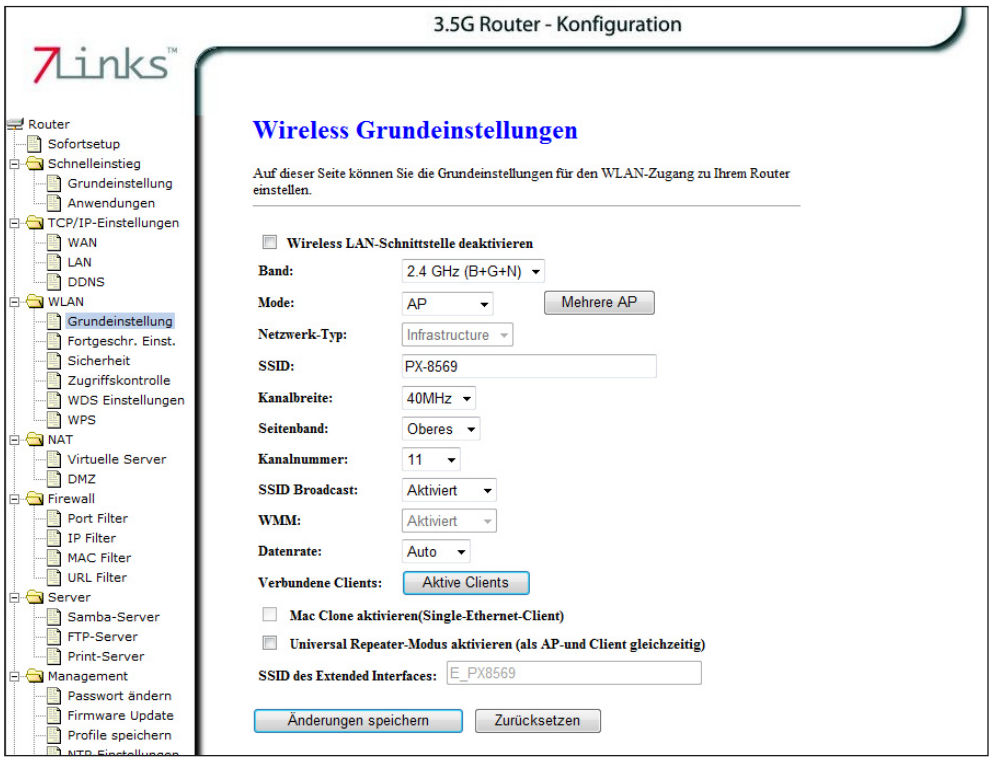


Speichern Sie die vorgenommenen Änderungen mit Klick auf **Änderungen speichern**.

Verwenden der MAC-Filterfunktion Whitelist

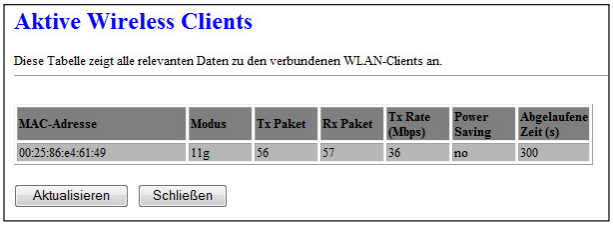
HINWEIS:
Der nächste Schritt kann nur ausgeführt werden, wenn der Router im Access-Point Modus eingestellt ist.

Die **Whitelist**-Filterfunktion für MAC-Adressen erlaubt nur ganz bestimmten, von Ihnen zugelassenen Geräten den Zugriff auf Ihr Netzwerk. Bevor Sie jedoch damit beginnen, diese Zugriffseinschränkung zu verwenden, sollten Sie zuerst einmal die MAC-Adressen aller Ihrer WLAN-Geräte zu notieren. Die einfachste Möglichkeit, die MAC-Adressen Ihrer Geräte zu ermitteln, besteht darin, alle Geräte, die künftig in Ihrem WLAN-Netzwerk genutzt werden sollen, nacheinander mit dem Router zu verbinden. Wenn Sie alle Geräte verbunden haben, klicken Sie im Hauptmenü der Routerkonfiguration auf **WLAN** und anschließend auf **Grundeinstellung**.

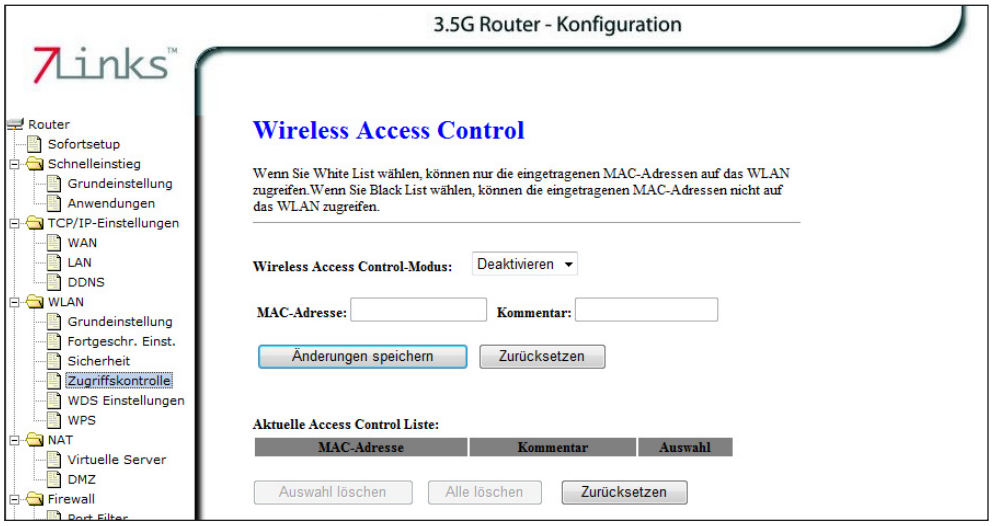


Klicken Sie nun auf den Button **Aktive Clients**.
In dieser Übersicht werden alle derzeit mit dem Router verbundenen Geräte mit Ihrer MAC-Adresse aufgelistet. Notieren Sie sich diese Adressen.

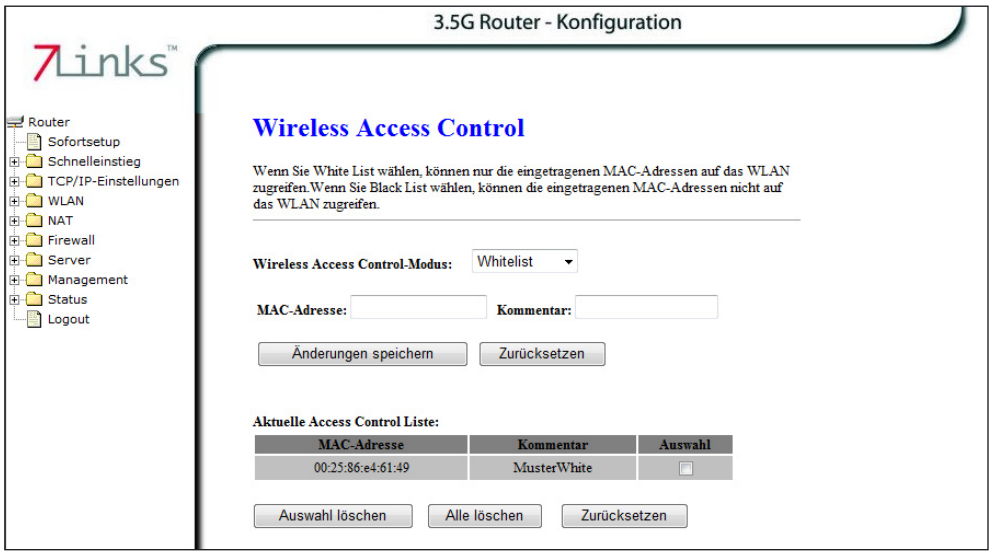
HINWEIS:
Oft sind die MAC-Adressen Ihrer WLAN-Geräte auch auf Aufklebern auf den Geräten selbst angebracht.



Schließen Sie das Fenster der Clientübersicht wieder.
Wählen Sie im Hauptmenü **WLAN** und den Unterpunkt **Zugriffskontrolle**.

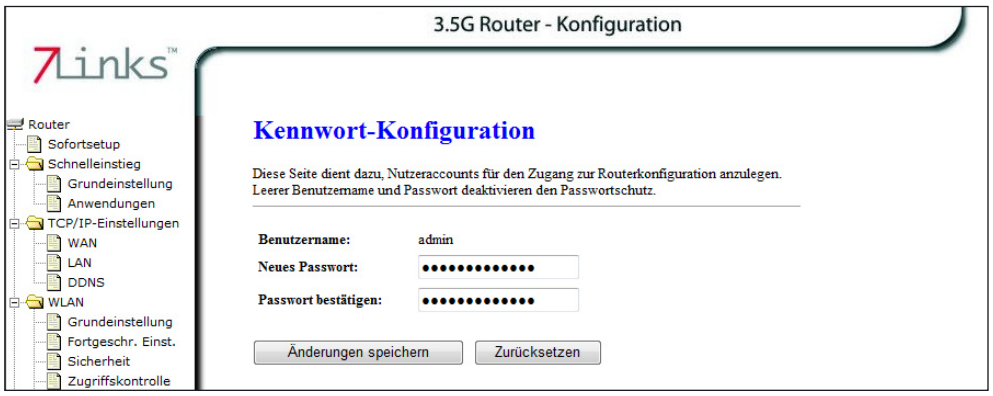


Stellen Sie nun den **Wireless Access Control-Modus** auf den Wert **Whitelist** ein.
Geben Sie nacheinander im Feld **MAC-Adresse** die MAC-Adresse Ihrer Geräte ein (ohne Doppelpunkte) und versehen Sie diese jeweils im Kommentarfeld mit einer sinnvollen Gerätebezeichnung (z.B. Notebook, Handy, usw.).
Speichern Sie jeden Eintrag mit Klick auf **Änderungen speichern**.



Den Router mit einem Passwort sichern

Um Ihren Router gegen unbefugten Zugriff auf die Konfigurationseinstellungen zu sichern, ist es notwendig, diesen mit einem Passwortschutz abzusichern.
Klicken Sie dazu im Hauptmenü der Routerkonfiguration auf **Management** und den Unterpunkt **Passwort ändern**.



Geben Sie nun ein neues Passwort für den Administratorzugang ein und bestätigen Sie dieses. Bestätigen Sie die Eingaben mit Klick auf **Änderungen speichern**.

HINWEIS:
Verwenden Sie möglichst nicht Ihren realen Namen als Benutzernamen und ein sicheres Passwort. Ein Passwort sollte möglichst aus mehr als 6 Zeichen und einigen Sonderzeichen (z.B. @, $, ?, !, usw.) bestehen. Notieren Sie sich das Passwort nötigenfalls und geben Sie dieses nicht an Außenstehende weiter.

ABSCHLIESSENDE WORTE

Sie haben Ihren neuen WLAN-Router nun in Ihr Netzwerk eingebunden und nach gängigen Sicherheitsmaßstäben gegen unbefugten Zugriff gesichert. Vielleicht sind Ihnen jedoch noch immer einige Begriffe oder Zusammenhänge aus dieser Anleitung unklar, oder nur in Ansätzen bekannt. Daher empfehlen wir Ihnen zur weiteren Lektüre über die Themen Netzwerke, WLAN und deren Sicherheit folgende Titel aus dem Sortiment unter www.pearl.de:

CL-945-675	Heimnetzwerke mit DSL & WLAN
PK-3915-675	Handbuch Heimnetzwerke

DETAILLIERTE ERLÄUTERUNGEN ZUR KONFIGURATION

SCHNELLKONFIGURATION

Schließen Sie den Router zur Vorbereitung per Kabel an einen einzelnen Rechner an. Rufen Sie dann über einen Webbrowser die Konfigurationsseite des Routers auf. Geben Sie dazu die werkseitige IP-Adresse des Routers ein (**192.168.1.1**).

Melden Sie sich als Administrator an, um zur Konfigurationsseite zu gelangen.
Benutzer: **admin**
Passwort: **admin**

Verwenden Sie den **Sofortsetup**-Assistenten, um die grundlegenden Einstellungen schnell und unkompliziert vorzunehmen.

Wählen Sie zuerst die Zeitzone, in der Sie sich befinden.
Legen Sie dann ein neues Administratorpasswort fest.
Den Geräte-Namen können Sie im nächsten Feld abändern (dient zur Identifikation des Routers im Samba -Modus).
Der vierte Schritt wird zur Konfiguration des WAN-Interface verwendet. Das Interface wird je nach Nutzungsart entweder per WAN-Port und Kabel, per UMTS/EDGE oder per WLAN verwendet. Geben Sie daher entsprechend der Anbindung die nötigen Informationen ein.
Der Punkt **WLAN-Setup** wird zur Konfiguration der WLAN-Schnittstelle verwendet.
Beim nächsten Punkt können Sie einen Verschlüsselungstyp für Ihr Netzwerk festlegen, jedoch sollten Sie bei der Vorkonfiguration darauf verzichten, um Fehlerquellen auszuschließen.
Die beiden übrigen Punkte werden für die Vorabkonfiguration nicht benötigt. Schließen Sie daher die Konfiguration mit **Änderungen speichern** ab.

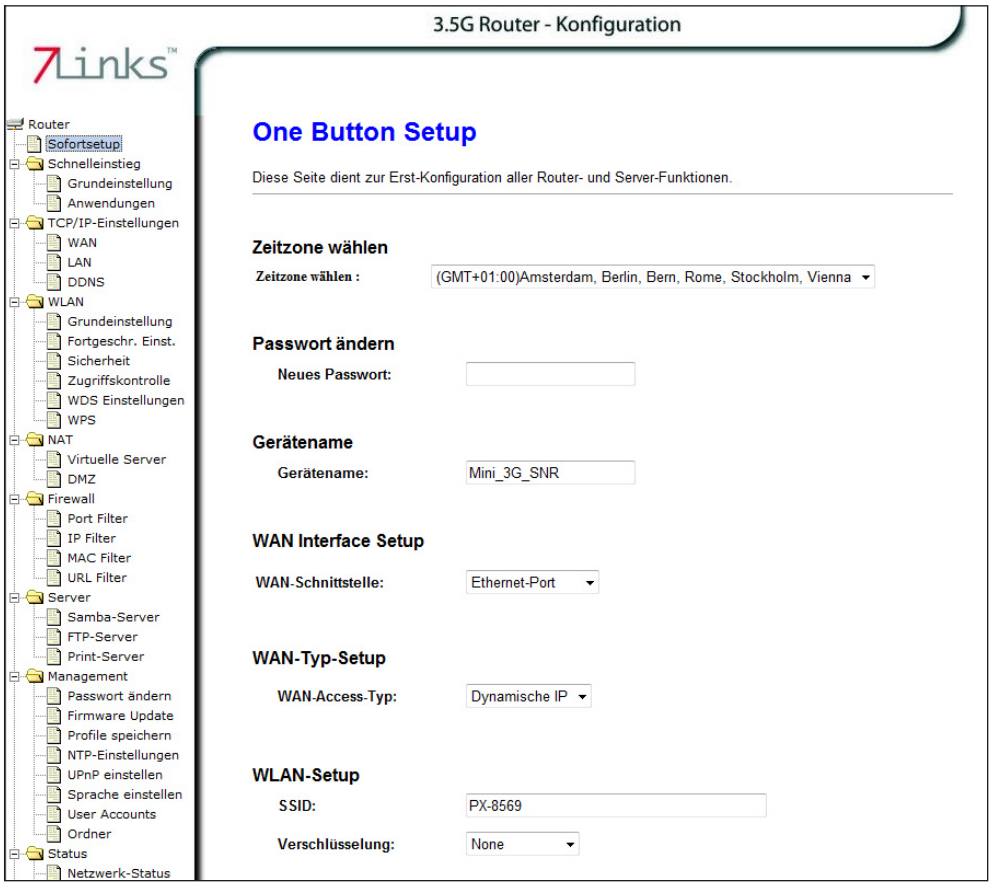
Nachdem Sie die Vorkonfiguration abgeschlossen haben, können Sie den Router am vorgesehenen Einsatzort anbringen.
Anschließend sollten Sie die endgültige Konfiguration vornehmen. Dies können Sie entweder per WLAN oder über den LAN-Zugang vornehmen.

SCHNELLREFERENZ DER KONFIGURATIONS-EINSTELLUNGEN MIT BEISPIELEN

Diese Referenz soll dem fortgeschrittenen Nutzer als Nachschlagewerk zu den einzelnen Menüpunkten und Einstellungsmöglichkeiten des WLAN-Routers dienen. Anwendungs- und Einsatzbeispiele geben dabei Aufschluss über mögliche Verwendungszwecke und veranschaulichen die einzelnen Vorgehensweisen.

SOFORT-SETUP

Sofort-Setup

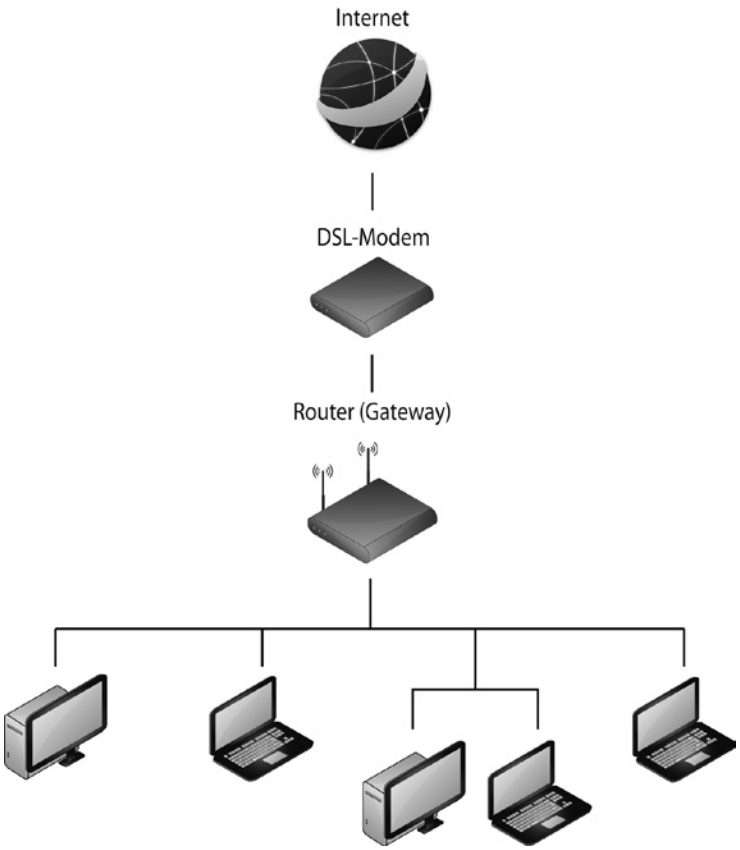


Option	Werte	Funktion
Zeitzone wählen	<parameter>	Die Zeitzone einstellen in der der Router steht.
Passwort ändern	<text>	Ändern des Passworts für den admin-Zugriff.
Gerätename	<text>	Bezeichnung des Routers (Samba-Zugriff).
WAN-Schnittstelle	Ethernet-Port Wireless 3.5G USB-Dongle	Festlegen der Zugriffsart auf die Internetverbindung.

Verschlüsselung	Keine WEP WPA WPA2	Anpassen an die Verschlüsselung, die der ISP verwendet.
Key Länge	64-Bit 128-Bit	Schlüssellänge für WEP-Verschlüsselung.
Key Format	Hex ASCII	Format des WEP-Schlüssels als ASCII (Klartext) oder in Hexadezimalen Ziffern.
Key Eingabe	<text> <hexcode>	Schlüssel, der für die WEP-Verschlüsselung verwendet wird.
WPA Cipher Suite	TKIP AES	Einstellen welche WPA/WPA2 Cipher verwendet werden.
Pre-Shared Key Format	Passwort Hex	Einstellen ob der Pre-Shared-Key im Klartext oder als Hex-Wert abgefragt wird.
Pre-Shared Key	<text> <hexcode>	Einstellen des verwendeten Passworts.
Service	UMTS/HSDPA/HSPA/HSUPA CDMA/CDMA 2000 TD_SCDMA	Einstellen des verwendeten Mobilfunkdienstes.
SIM-Karten PIN	<text> Keine	Eingabe der PIN der SIM-Karte des UMTS-Sticks oder, wenn **Keine** gewählt wird, wird keine PIN verwendet.
PIN bestätigen	<text>	Nochmalige Eingabe der PIN.
APN	<text>	Eingabe des APN-Namens des ISP.
Benutzername	<text>	Eingabe des ISP-Benutzernamens.
Passwort	<text>	Eingabe des ISP-Benutzerpassworts.
Telefon	<text>	Eingabe der GPRS-Einwahlsequenz (Standard: ***99***1#**).
SSID	<text>	Eingabe der zu verwendenden SSID der WLAN-Schnittstelle des Routers.
Verschlüsselung	Keine WEP WPA WPA2 WPA2 Mixed	Legt fest welche Sicherheitsstufe der WLAN-Verschlüsselung verwendet werden soll.
Key Eingabe	<hexcode>	Eingabe des zu verwendenden WEP-Schlüssels für das WLAN.
Pre-Shared Key	<text>	Einstellen des verwendenden Passworts.

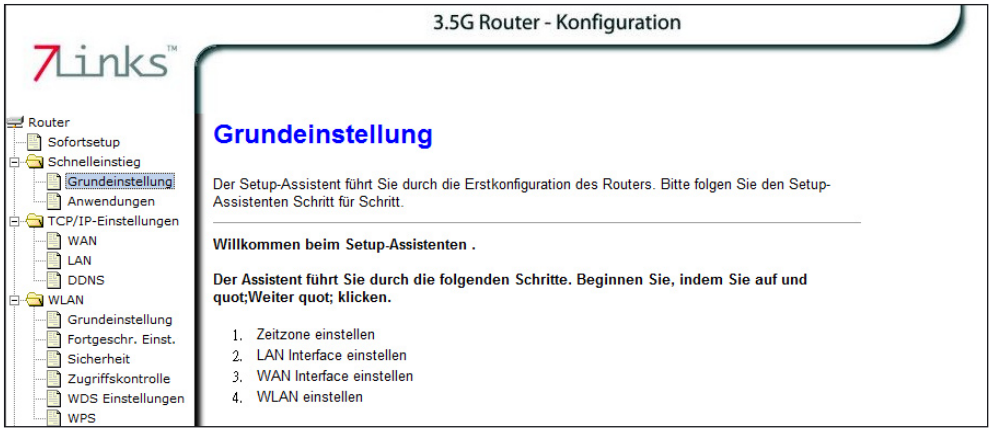
USB-Datenträger formatieren	Ja Nein	Einstellen, ob der angeschlossene USB-Datenträger formatiert werden soll.
Typ	FAT NTFS EXT3	Einstellen in welchem Dateisystem der USB-Datenträger formatiert werden soll.
Benutzername	<text>	Festlegen eines Nutzers mit diesem Namen.
Passwort	<text>	Festlegen des Passworts für den Nutzer.
FTP-Server	Ja Nein	FTP-Verwendung durch den Nutzer erlauben.

Beispiele



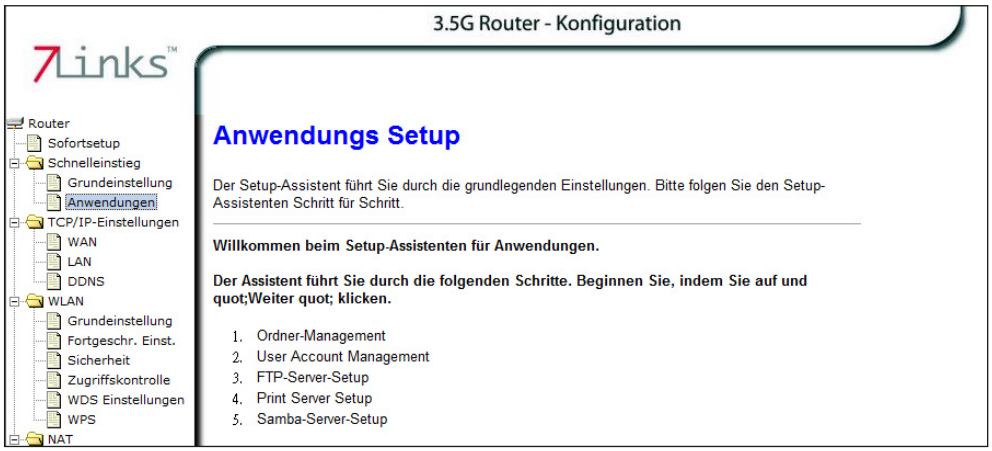
SCHNELLEINSTIEG

Grundeinstellung



Option	Werte	Funktion
Zeitzonen-Einstellung	<parameter>	Festlegen der Zeitzone und des NTP-Servers. Siehe auch S.65.
LAN Interface Setup	<parameter>	Festlegen der LAN-IP-Adresse und der Samba-Bezeichnung.
WAN Interface Setup	<parameter>	Festlegen der Verbindung zum Internet. Siehe auch S.39.
Wireless Grundeinstellungen	<parameter>	Festlegen der SSID und der Verschlüsselung. Siehe auch S. 46.

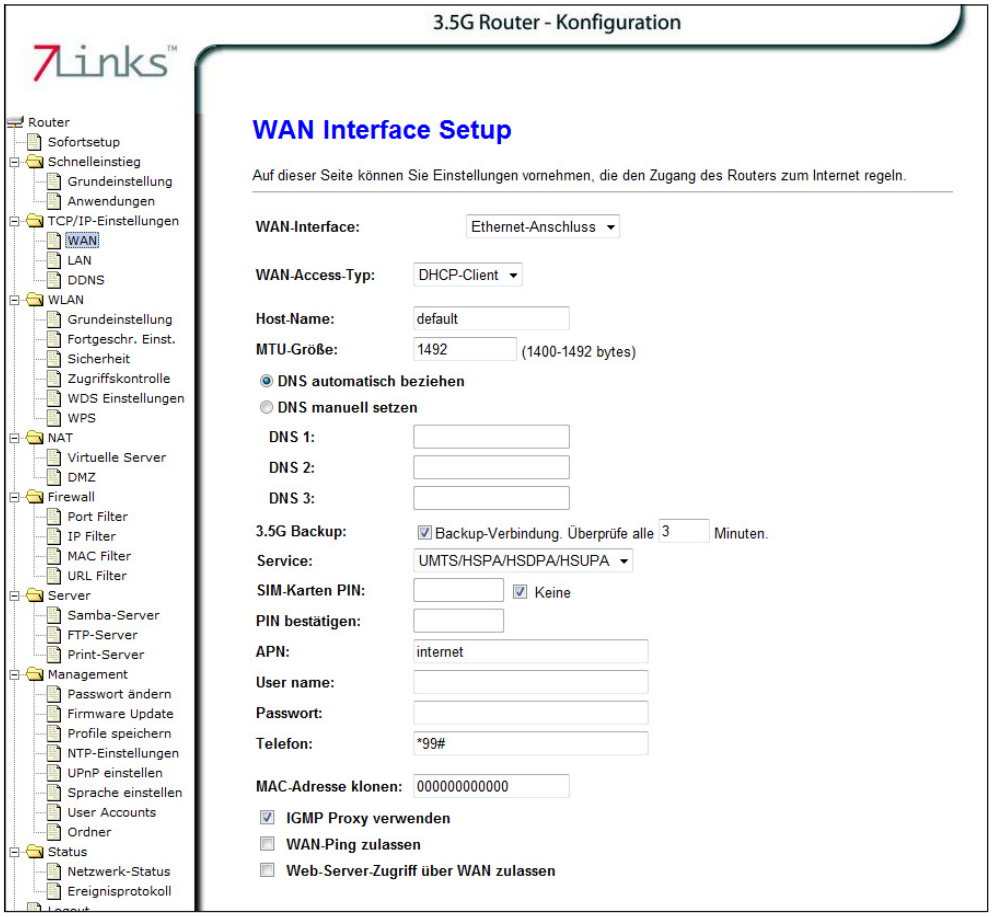
Anwendungen



Option	Werte	Funktion
Anwendungs-Setup	<parameter>	Verwalten von angeschlossenen USB-Speichern. Siehe auch S.67.
User Account Management	<parameter>	Verwalten von FTP-Freigaben. Siehe auch S.66.
FTP-Server	<parameter>	Einstellungen zum FTP-Server. Siehe auch S.61
Print Server	<parameter>	Einstellungen zum Print-Server. Siehe auch S.62.
Samba-Server-Einstellung	<parameter>	Einstellungen zur Samba-Server Funktionalität. Siehe auch S.60.

TCP/IP EINSTELLUNGEN

WAN Schnittst.



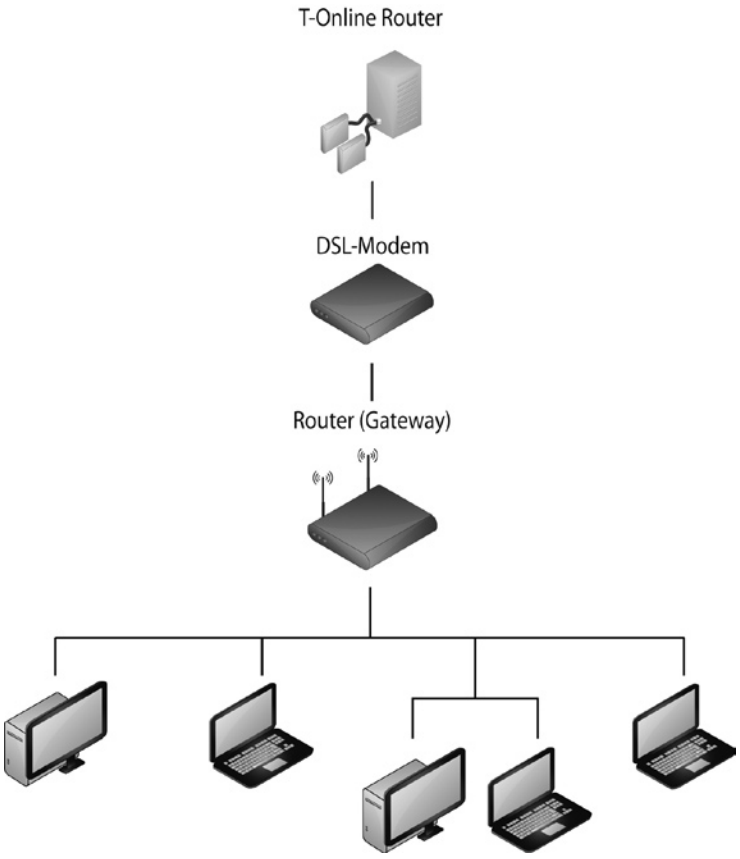
Option	Werte	Funktion
WAN-Interface	Ethernet-Anschluss Wireless 3.5G-USB-Dongle	Einstellen des Verbindungstyps der WAN-Schnittstelle.
Verschlüsselung	Keine WEP WPA WPA2	Verschlüsselungstyp des ISP.
Key Length	64-Bit 128-Bit	Länge des WEP-Schlüssels.
Key Format	Hex ASCII	Verwendetes Schlüsselformat.
Key Setting	<text> <hexcode>	Eingabe des ISP-Schlüssels.
WPA Cipher Suite	TKIP AES	Verwendete Verschlüsselungstechnik.
Pre-Shared Key Format	Passwort Hex	Verwendete Schreibweise des Schlüssels.

Pre-Shared Key	<text> <hexcode>	Eingabe des ISP-Passworts/ Schlüssels.
WAN-Access-Typ	Statische IP DHCP Client PPPoE PPTP	Einstellen der IP-Bezugsquelle der WAN-Schnittstelle.
IP-Adresse	<text>	IP-Adresse, mit der der Router über die WAN-Schnittstelle angesprochen werden kann.
Subnetzmaske	<text>	Zu verwendende Subnetzmaske.
Standard Gateway	<text>	Zu verwendendes Gateway. IP-Adresse des ISP.
MTU Größe	1360-1500	Maximale Packetgröße. DHCP-Standard: **1492**, Statische IP: **1500**
Host Name	<text>	Bezeichnung des Routers.
Benutzername	<text>	Benutzername zur Anmeldung beim ISP.
Passwort	<text>	Passwort zur Anmeldung beim ISP.
Service Name	<text>	Dialstring (falls erforderlich).
Connectiontyp	Kontinuierlich Connect on Demand Manuell	Art des Verbindungsaufbaus.
Idle Time	1-1000	Zeit bis zum Verbindungsabbruch, wenn kein Datenverkehr mehr stattfindet.
MPPE Verschlüsselung anfordern	Ein Aus	Microsoft Punkt-zu-Punkt-Verschlüsselung verwenden.
Service	UMTS/HSDPA/ HSPA/ HSUPA CDMA/CDMA2000 TD-SCDMA	Verwendeter Funkstandard.
SIM-Karten PIN	<text> Keine	PIN der verwendeten SIM-Karte oder Keine, wenn die PIN-Abfrage der Karte deaktiviert ist.
PIN bestätigen	<text>	Wiederholen der PIN zur Sicherheit.
APN	<text>	APN des Mobilfunkproviders.
Benutzername	<text>	Benutzername beim Mobilfunkprovider.
Passwort	<text>	Passwort beim Mobilfunkprovider.
Telefon	<text>	GPRS Einwahlsequenz (in Deutschland meist ***99***1#**).

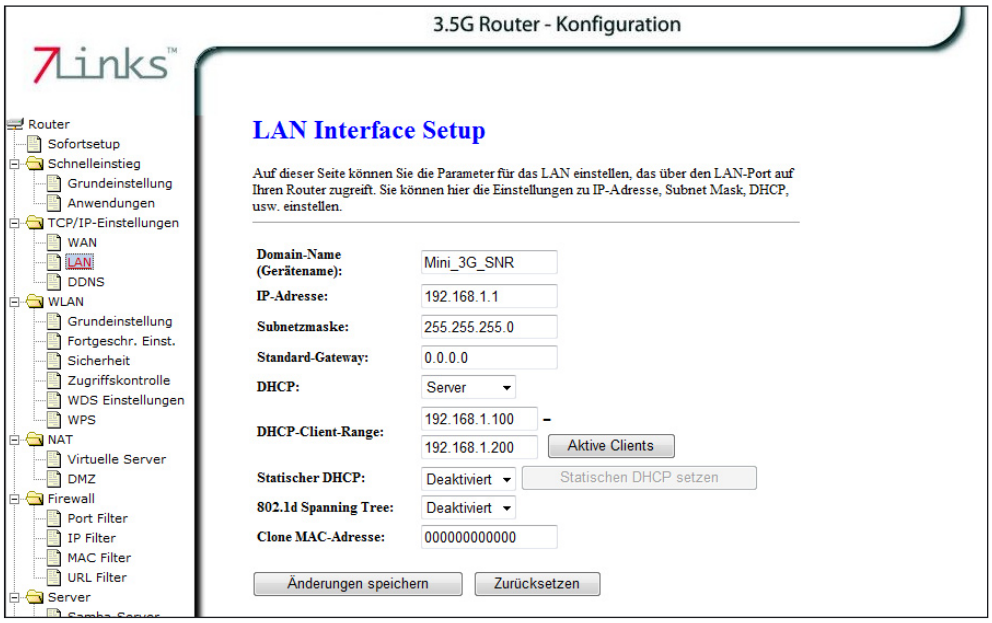
DNS automatisch beziehen	Ein Aus	Beziehen der DNS-IPs vom Gateway.
DNS manuell einstellen	Ein Aus	Manuelle Angabe der DNS-IPs.
DNS 1-3	<text>	IP-Adressen der zu verwendenden DNS-Server.
Clone MAC Adresse	<text>	MAC-Adresse, die für das „cloning“ extern verwendet werden soll.
Immer	An Aus	Ständige Verbindung zum ISP.
Idle	<text>	Zeit nach der die Verbindung getrennt wird (ohne erkennbaren Traffic).
Manuell	An Aus Trennen	Manueller Verbindungsaufbau und Trennung.
IGMP Proxy verwenden	Ein Aus	Multicast Proxy einschalten.
Ping Access on WAN verwenden	Ein Aus	Ping-Anfragen auf den Router erlauben.
Web Server Access on WAN	Ein Aus	Webserver-Anfragen vom WAN aus erlauben.

Beispiele

Beispiele

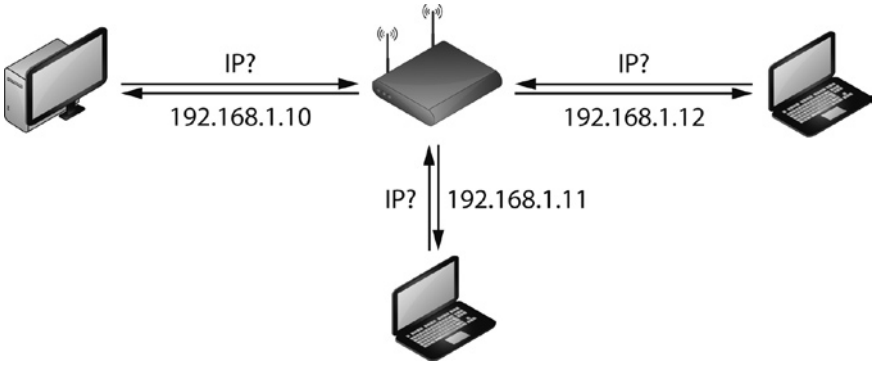


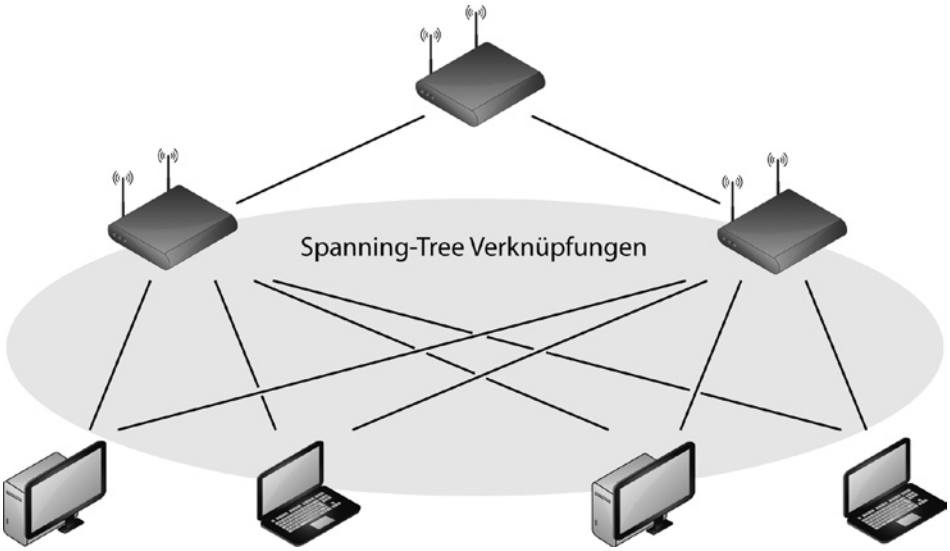
LAN Schnittst.



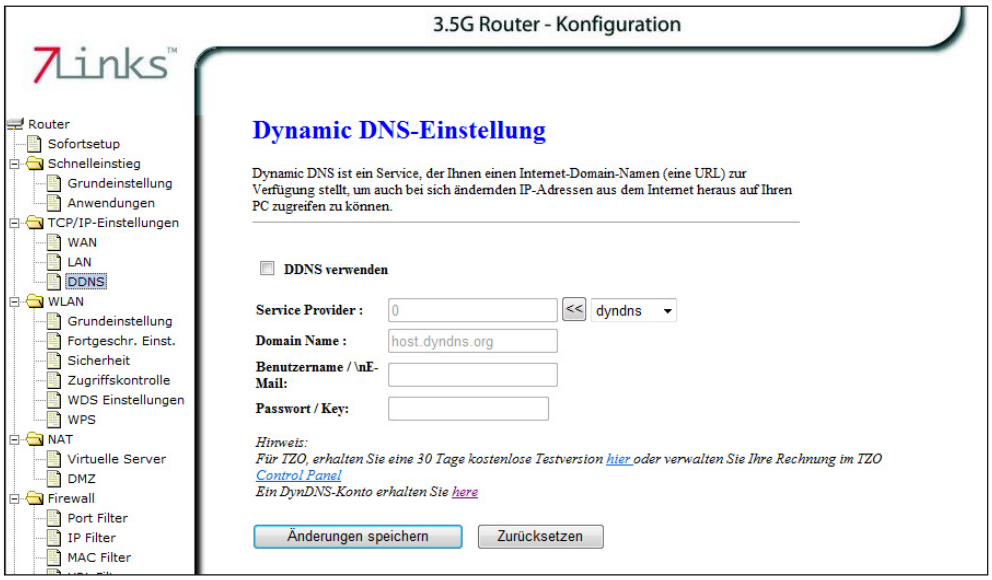
Option	Werte	Funktion
Domain Name	<text>	Einstellen des Namens innerhalb der Domäne.
IP-Adresse	<text>	IP-Adresse, mit der der Router über die LAN-Schnittstelle angesprochen werden kann.
Subnetzmaske	<text>	Zu verwendende Subnetzmaske.
Standard Gateway	<text>	Zu verwendendes Gateway. Entweder IP-Adresse des ISP oder des Hauptrouters.
DHCP	Deaktiviert Client Server	Regelt die Verwendung von DHCP über den Router (automatische IP-Adressen Vergabe).
DHCP-Client Range	<text> <text>	Einstellen des zu vergebenden IP-Adressbereichs.
Statischer DHCP	Akitivert Deaktiviert Statischen DHCP setzen	Vergabe von statischen IP-Adressen an bestimmte MAC-Adressen innerhalb des Netzwerks per DHCP (z.B. für Server).
802.1d Spanning Tree	Ein Aus	Verwendung des Spanning Tree Protokolls.
Clone MAC Address	<hexcode>	MAC-Adresse, die für das „cloning“ intern verwendet werden soll.

Beispiele


IP?
192.168.1.10
IP?
192.168.1.12
IP?
192.168.1.11

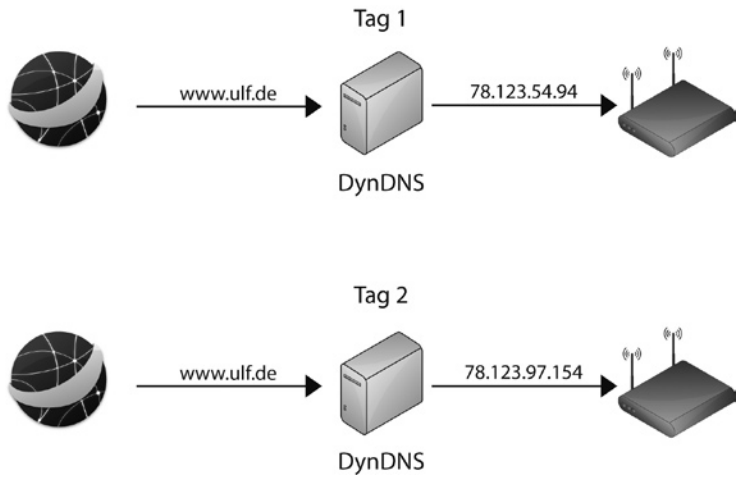

Spanning-Tree Verknüpfungen

DDNS



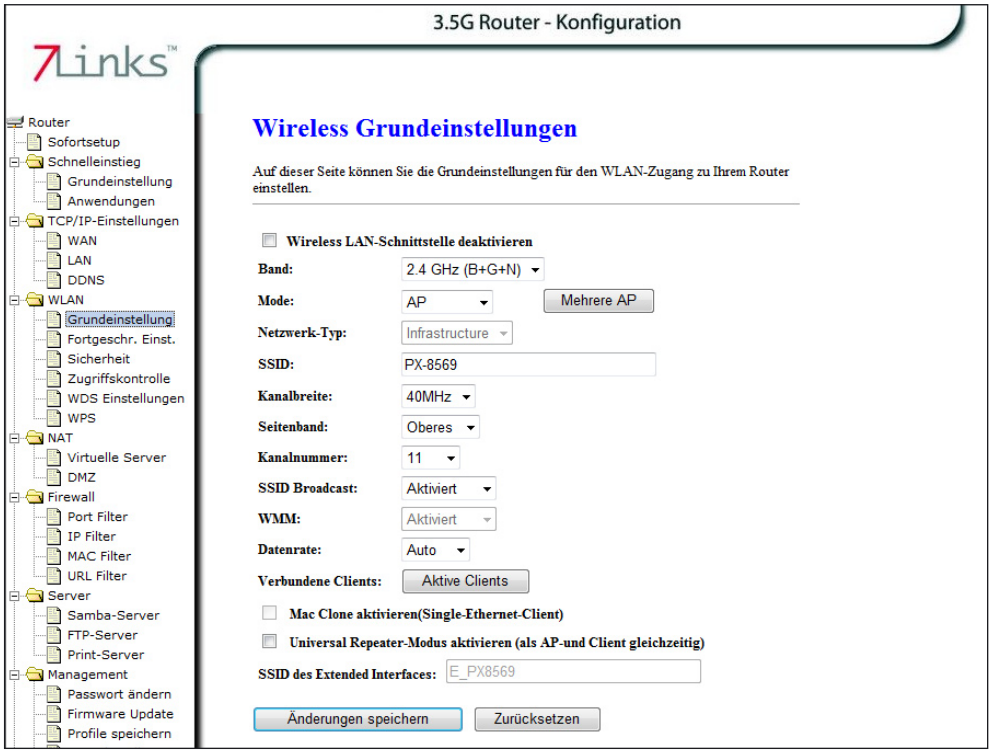
Option	Werte	Funktion
DDNS verwenden	Ein Aus	Dynamisches DNS verwenden.
Service Provider	DynDNS Tzo Changeip Eurodns Ovh No-ip Ods regfish	Auswahl des DDNS-Serviceanbieters.
Domain Name	<text>	Zu verwendende Domainbezeichnung.
Benutzer Name/ E-Mail	<text>	Benutzerkennung beim DDNS-Anbieter.
Passwort/Key	<text>	Benutzerpasswort beim DDNS-Anbieter.

Beispiel



WIRELESS

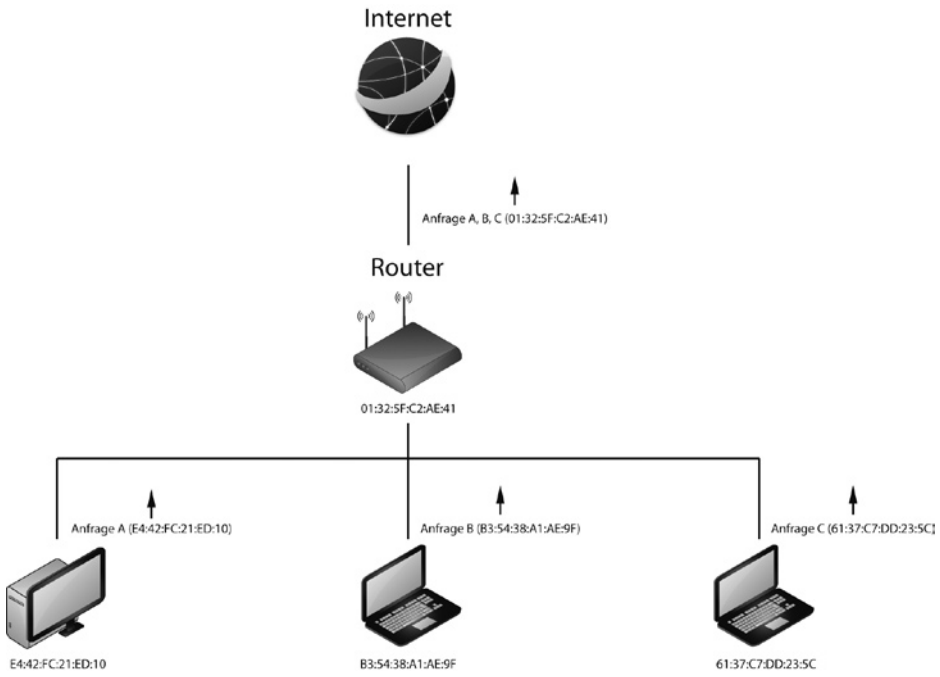
Grundeinstellungen

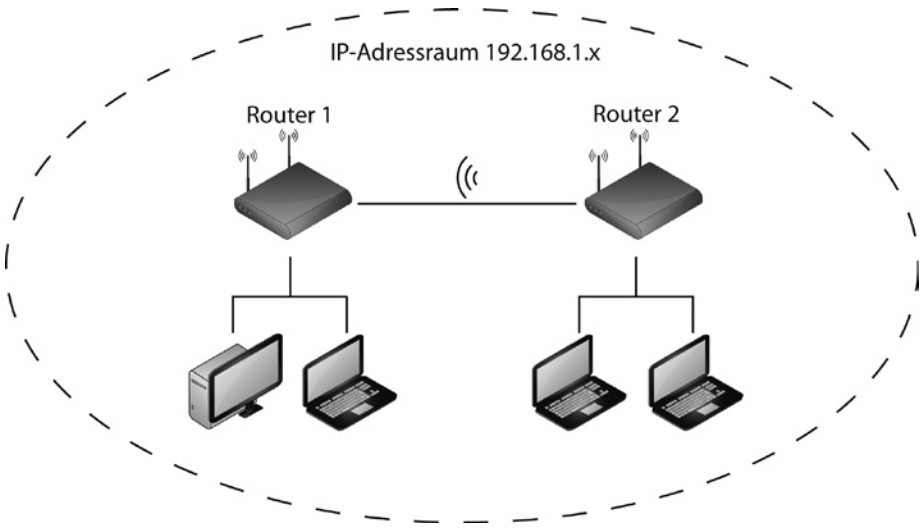


Option	Werte	Funktion
Wireless LAN-Schnittstelle deaktivieren	Ein Aus	Aktiviert oder deaktiviert die WLAN-Funktion des Routers.
Band	2,4 GHz (B) 2,4 GHz (G) 2,4 GHz (N) 2,4 GHz (B+G) 2,4 GHZ (G+N) 2,4 GHZ (B+G+N)	Einstellung der verwendeten WLAN-Bänder.
Mode	AP Client WDS AP+WDS	Konfigurieren der Verwendungsart der WLAN-Schnittstelle. Bei einem **Wireless ISP** muss **Client** aktiviert sein.
Netzwerk Typ	Infrastruktur Ad Hoc	Feste oder variable Netzwerkstruktur
SSID	<text>	Bezeichnung des Netzwerks
Kanalnummer	Auto 1-13	Kanal der für WLAN verwendet werden soll
SSID Broadcast	Aktiviert Deaktiviert	Übermittlung der SSID.

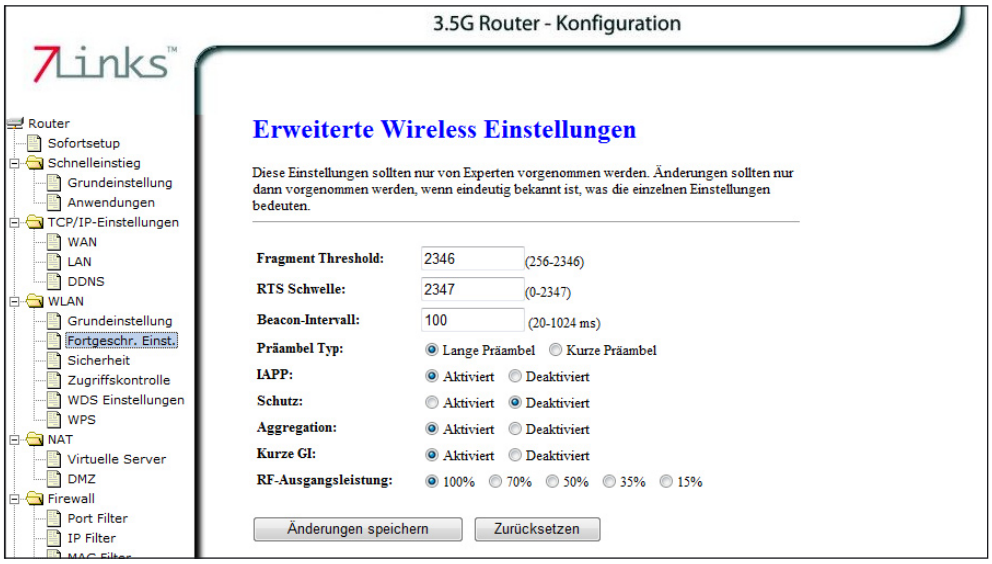
Datenrate	<parameter>	Zu verwendene Datenrate (Standard: Auto).
Mac Clone verwenden	Ein Aus	Vergleichbar mit NAT, werden im Netzwerk befindliche Geräte nach „außen“ mit der gleichen MAC-Adresse dargestellt.
Universal Repeater Modus verwenden	Ein Aus	Wenn dieser Punkt aktiv ist, agiert die WLAN-Schnittstelle gleichzeitig im AP und Client Modus. Diese Einstellung ist spezielle für den Einsatz als im **Wireless ISP**-Modus von Bedeutung.
SSID des Extended Interfaces	<text>	Bezeichnung des erweiterten Netzwerks, wenn der **Universal Repeater Modus** verwendet wird.

Beispiele





Fortgeschr. Einst.



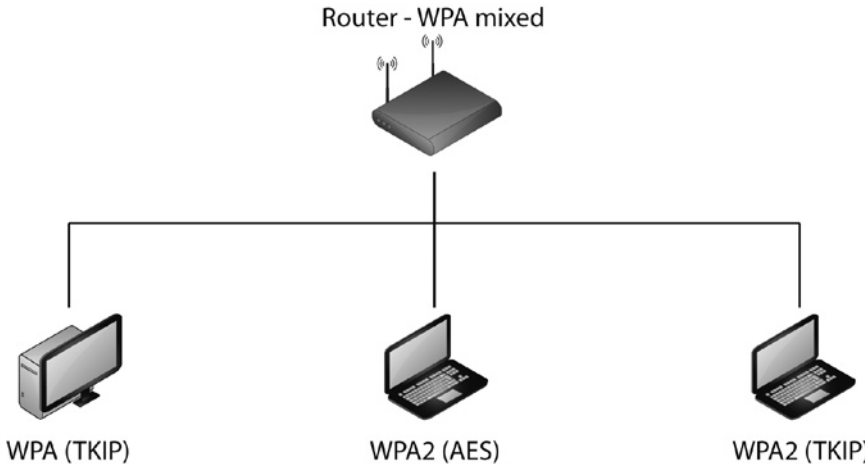
Option	Werte	Funktion
Fragement Threshold	256-2346	Fragmentierungsschwellwert der verwendeten Datenpakete. Bei schlechter Verbindung kann ein niedrigerer Wert die Übertragungsqualität verbessern.
RTS Schwelle	0-2347	Schwellwert für Handshake-Anfragen zur Kollisionsvermeidung.
Beacon Intervall	20-1024	Synchronisationsintervall der WLAN-Schnittstelle.
Präambel Typ	Lang Kurz	Größe der CRC-Datenpakete.
IAPP	Ein Aus	Verwenden des **Inter Access Point Protokolls** (Roaming zwischen Access-Points)
Schutz	Ein Aus	Wenn aktiviert, können sowohl 802.11b als auch 802.11g Geräte im gleichen Netzwerk verwendet werden.
Aggregation	Ein Aus	Zusammenfassen von Routen erlauben.
Kurze GI	Ein Aus	Verwendung von kurzen Binärpräfixen.
RF-Ausgangsleistung	100% 70% 50% 35% 15%	Einstellung der Sendeleistung der integrierten Antenne. Schwächere Leistung kann die Sicherheit des Netzwerks erhöhen (kein WLAN-Empfang außerhalb des Gebäudes).

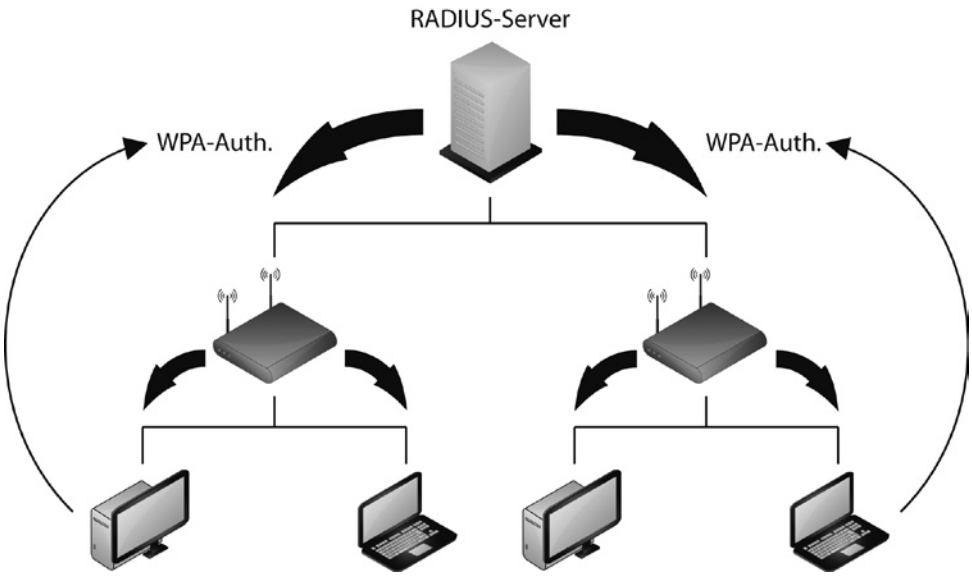
Sicherheit

Option	Werte	Funktion
SSID auswählen	<parameter>	Auswahl des Netzwerks für das die Sicherheitseinstellungen angepasst werden sollen.
Verschlüsselung	Keine WEP WPA WPA2 WPA Mixed	Einstellen der verschiedenen Verschlüsselungsmethoden. Wird **WEP** verwendet, können unter **Set WEP Key** die Schlüssel eingestellt werden.
802.1x Authentifizierung verwenden	Ein Aus 64 Bit 128 Bit	Einstellen der Schlüssellänge bei der Verwendung von **WEP** mit einem Radius Server.
Authentifizierung	Offenes System Shared Key Auto	Authentifizierungsmethode bei WEP-Verschlüsselung.
Key Lenght	64 Bit 128 Bit	Einstellen der Schlüssellänge für WEP.
Key Format	Hex ASCII	Einstellen ob der WEP-Key im Klartext oder als Hex-Wert abgefragt wird.
Encryption Key	<text> <hexcode>	Eingabe des WEP-Schlüssels.
WPA Authentifizierungs Methode	Enterprise Personal	Einstellen, ob ein RADIUS-Server verwendet wird, oder die Authentifzierung per Pre-Shared-Key vorgenommen werden soll.
WPA Cipher Suite	TKIP AES	Einstellen welche WPA Cipher verwendet werden.
WPA2 Cipher Suite	TKIP AES	Einstellen welche WPA2 Cipher verwendet werden.

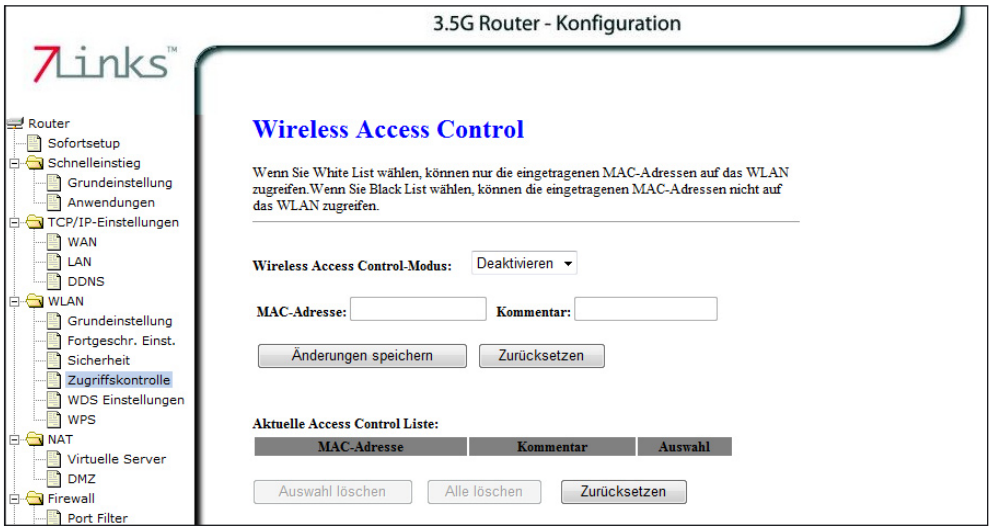
Pre-Shared Key Format	Passphrase Hex	Einstellen ob der Pre-Shared-Key im Klartext oder als Hex-Wert abgefragt wird.
Pre-Shared Key	<text> <hexcode>	Einstellen des verwendeten Schlüssels.
RADIUS-Server IP-Adresse	<text>	Verbindungsdaten des verwendeten RADIUS-Servers.
RADIUS Server-Port	<text>	Port auf dem der RADIUS-Server erreicht wird.
RADIUS-Server-Passwort	<text>	Eingabe des Passworts für den RADIUS-Server.

Beispiele





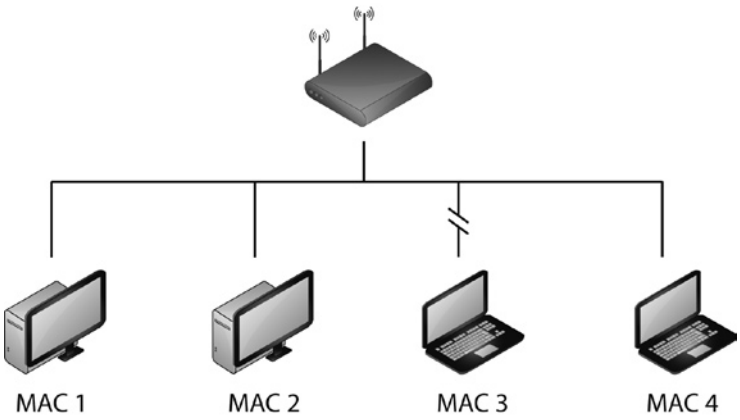
Zugriffskontrolle



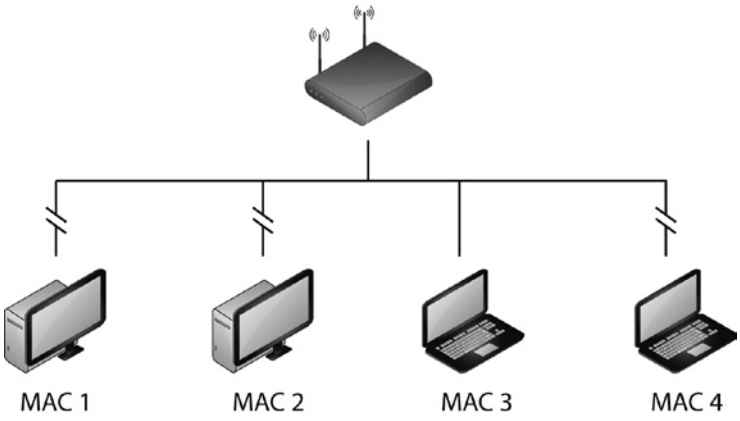
Option	Werte	Funktion
Wireless Access Control-Modus	Deaktivieren White List Black List	Einstellen der verwendeten Zugangskontrolle.
MAC-Adresse	<text>	Die betreffende MAC-Adresse.
Kommentar	<text>	Kommentar.

Beispiele

Router (Blacklist: MAC 3)



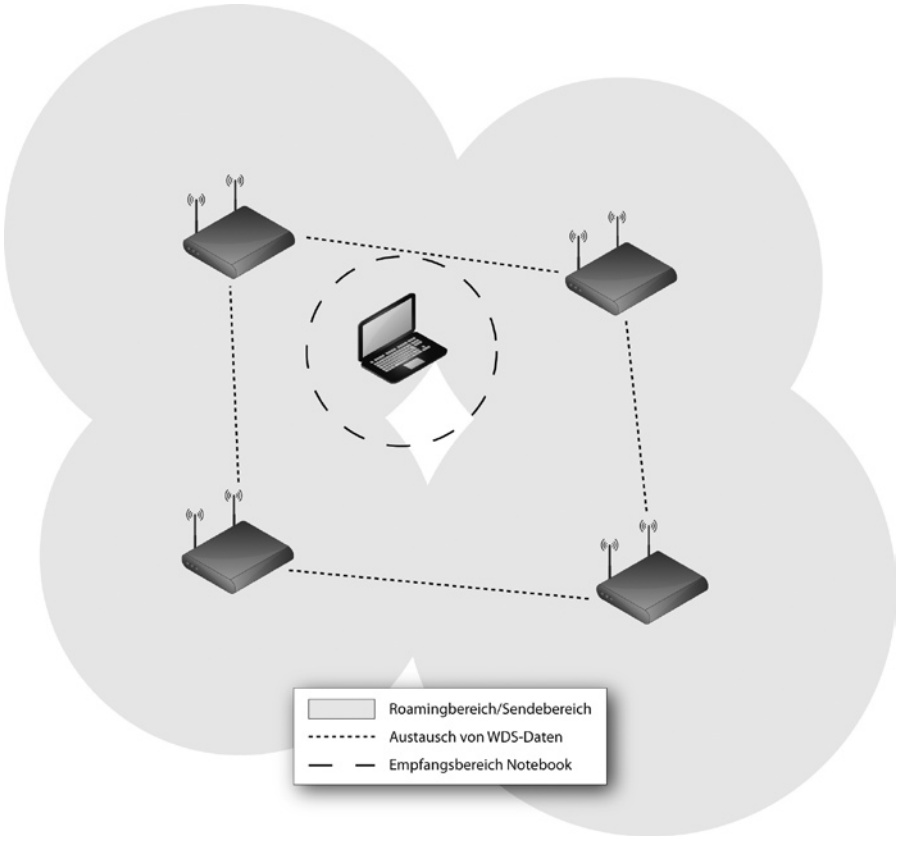
Router (Whitelist: MAC 3)



WDS Einstellungen

Option	Werte	Funktion
WDS verwenden	Ein Aus	Aktivieren des Wireless Distribution Systems (verteilte Access-Points).
MAC-Adresse	<text>	MAC-Adresse eines Access-Points.
Datenrate	Auto <parameter>	Einstellen der zu verwendenden Datenübertragungsrate (Bandbreite).
Kommentar	<text>	Kommentar.

Beispiel

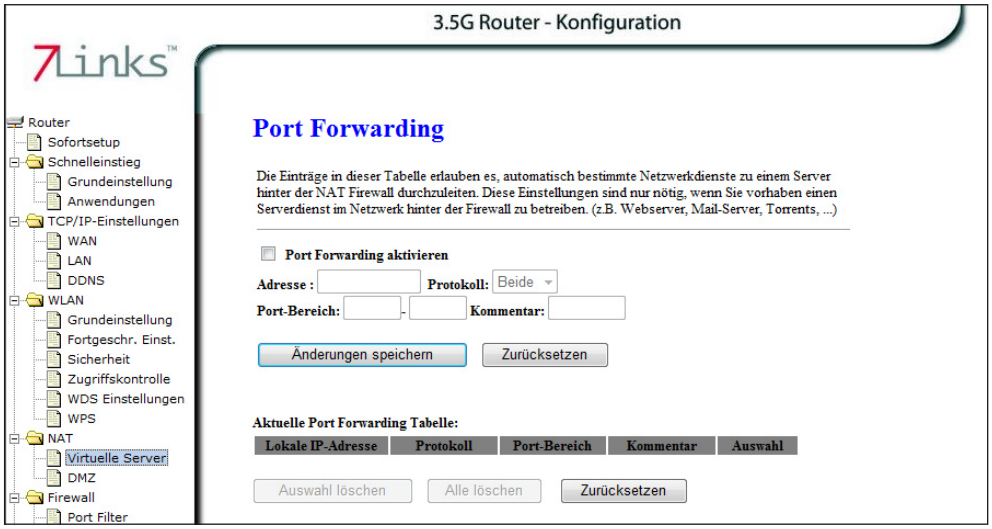


WPS

Option	Werte	Funktion
WPS deaktivieren	Ein Aus	Aktivieren des WiFI Protected Setups zur einfachen Integration von Wireless Geräten.
Client PIN	<text>	PIN, die von Clients verwendet wird.

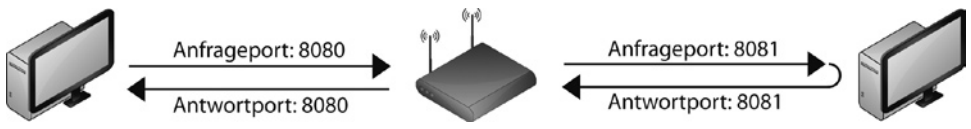
NAT

Port Forwarding



Option	Werte	Funktion
Port Forwarding aktivieren	Ein Aus	Forwarding aktivieren.
Adresse	<text>	Für diese IP-Adresse anwenden.
Protokoll	Beide TCP UDP	Auf diese/s Protokoll/e anwenden.
Port-Bereich	<text> <text>	Für diese Ports anwenden.
Kommentar	<text>	Kommentar.

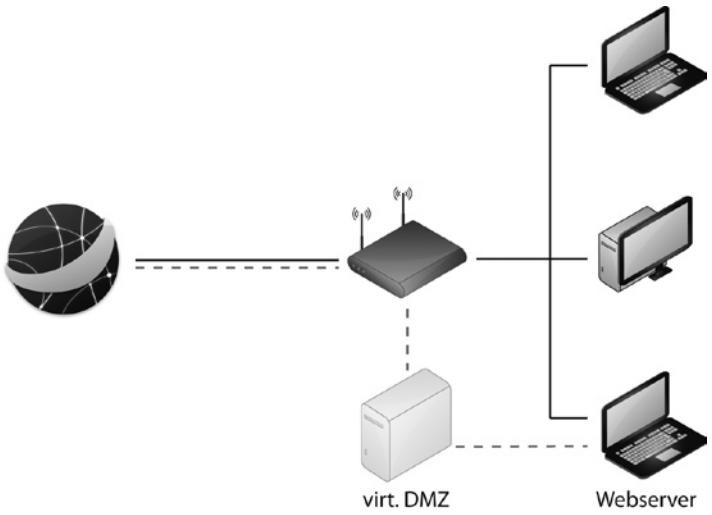
Beispiel



DMZ

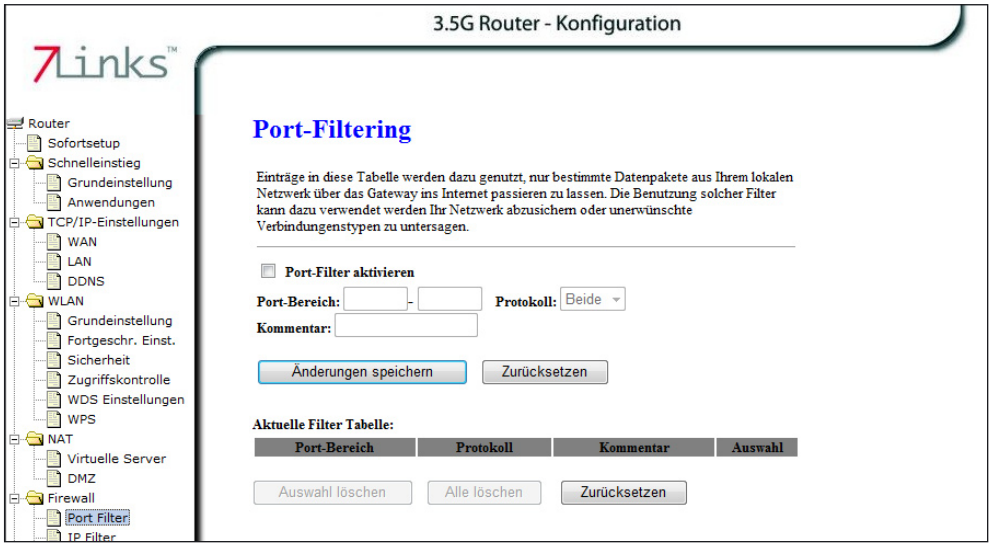
Option	Werte	Funktion
DMZ aktivieren	Ein Aus	Virtuelle DMZ konfigurieren.
DMZ Host IP-Adresse	<text>	IP-Adresse des zu verwendenden virtuellen DMZ-Servers.

Beispiel



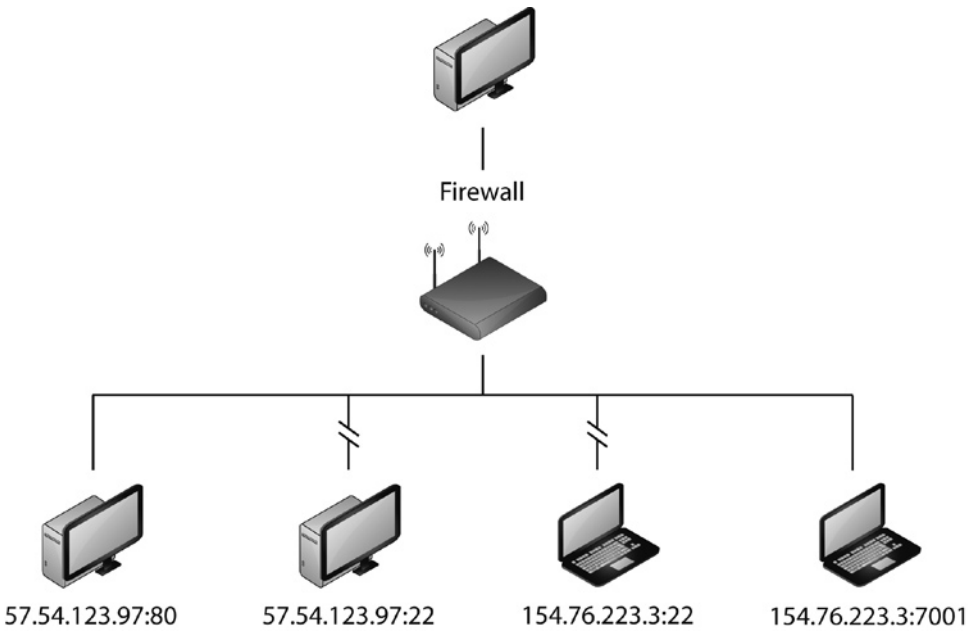
FIREWALL

Port Filter



Option	Werte	Funktion
Port Filtering aktivieren	Ein Aus	Filter aktivieren.
Port-Bereich	<text> <text>	Auf diese Ports anwenden.
Protokoll	Beide TCP UDP	Auf diese/s Protokoll/e anwenden.
Kommentar	<text>	Kommentar.

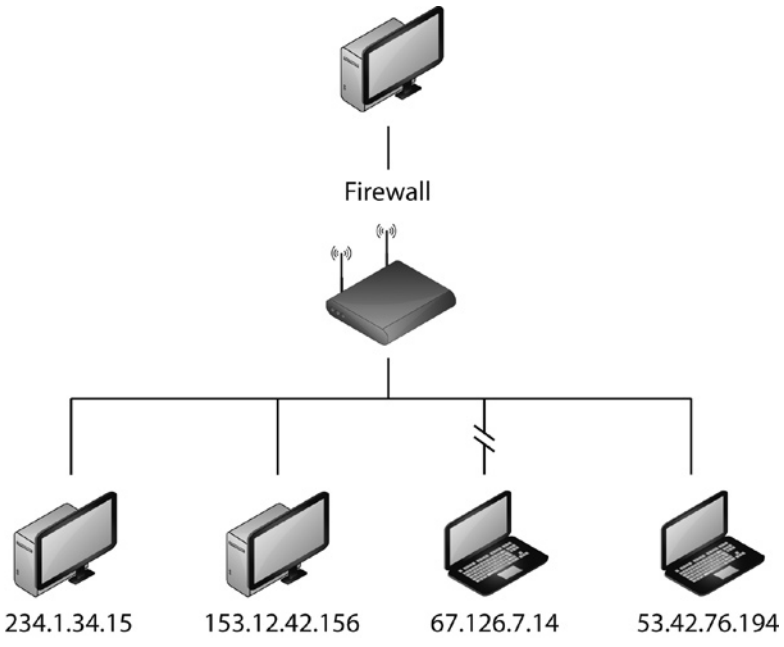
Beispiel



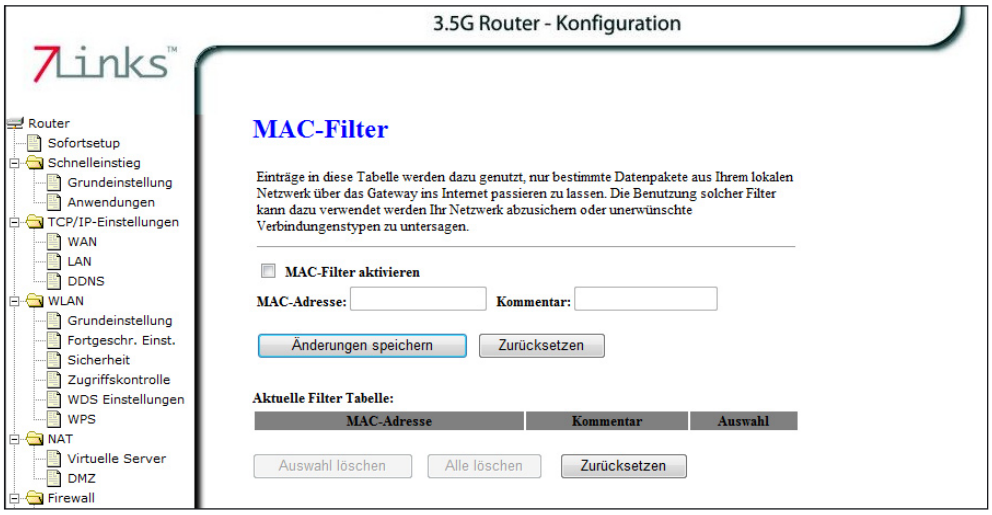
IP Filter

Option	Werte	Funktion
IP-Filter aktivieren	Ein Aus	Filter aktivieren.
Lokale IP-Adresse	<text>	Für diese IP-Adresse anwenden.
Protokoll	Beide TCP UDP	Auf diese/s Protokoll/e anwenden.
Kommentar	<text>	Kommentar.

Beispiel

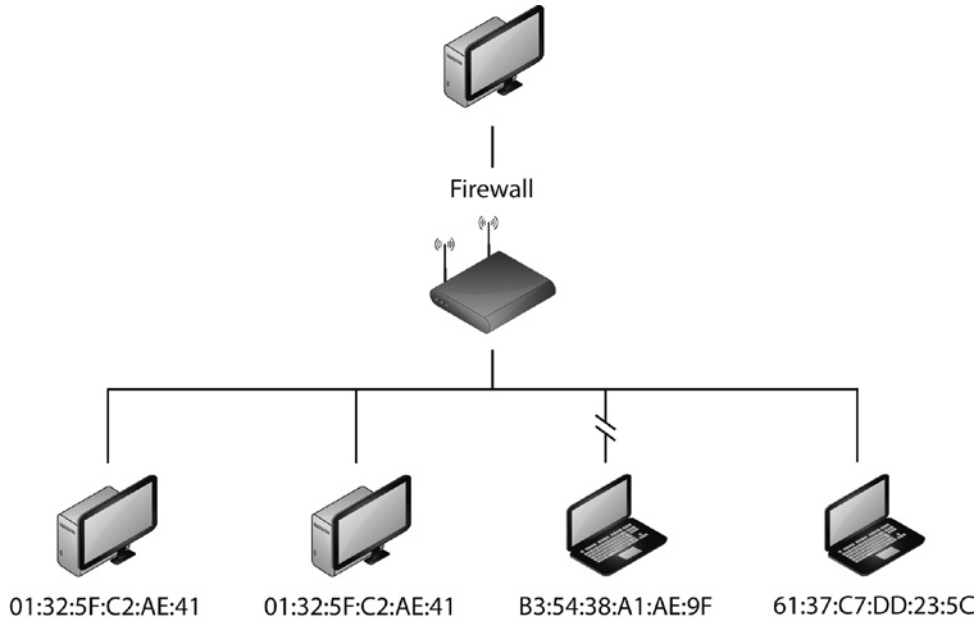


MAC Filter

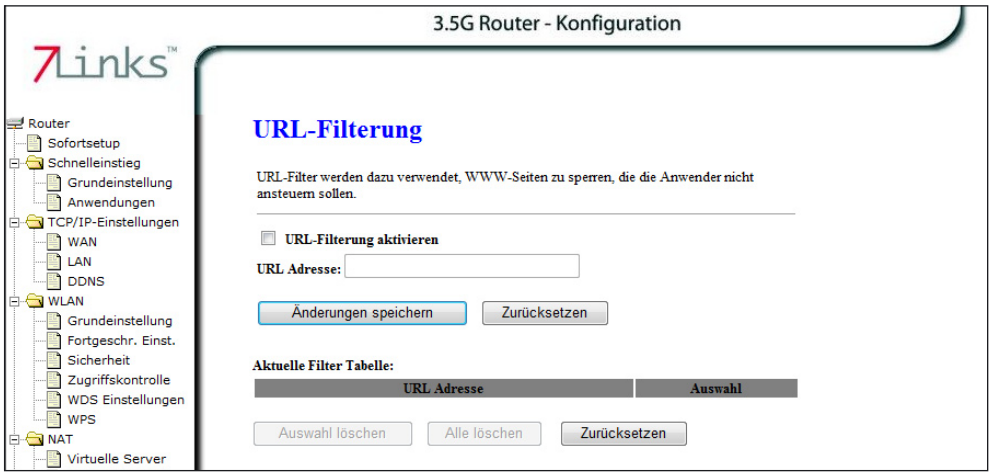


Option	Werte	Funktion
MAC-Filter aktivieren	Ein Aus	Filter aktivieren.
MAC-Adresse	<text>	Für diese MAC-Adresse anwenden.
Kommentar	<text>	Kommentar.

Beispiel

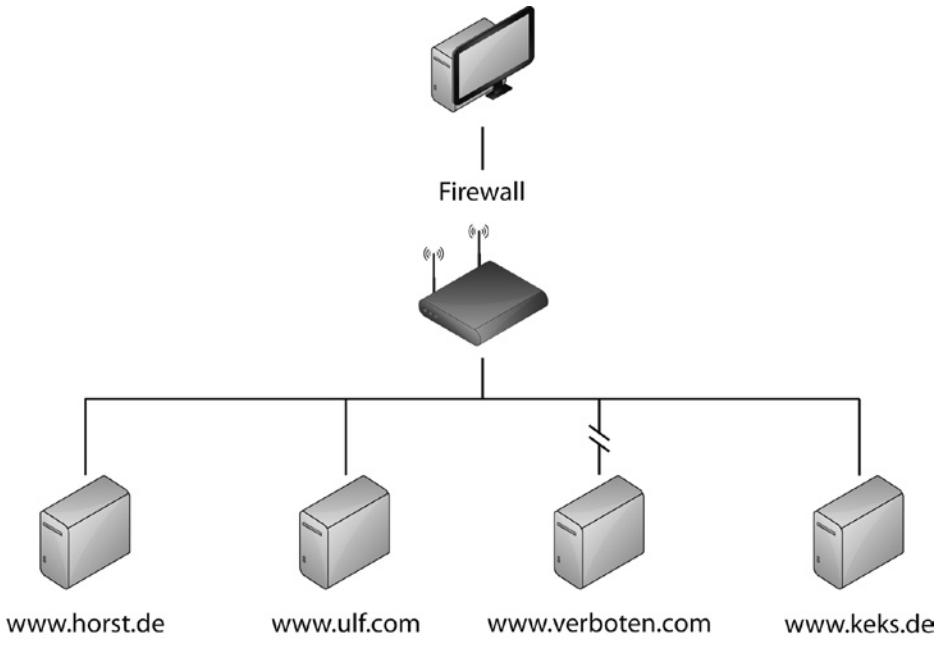


URL-Filter



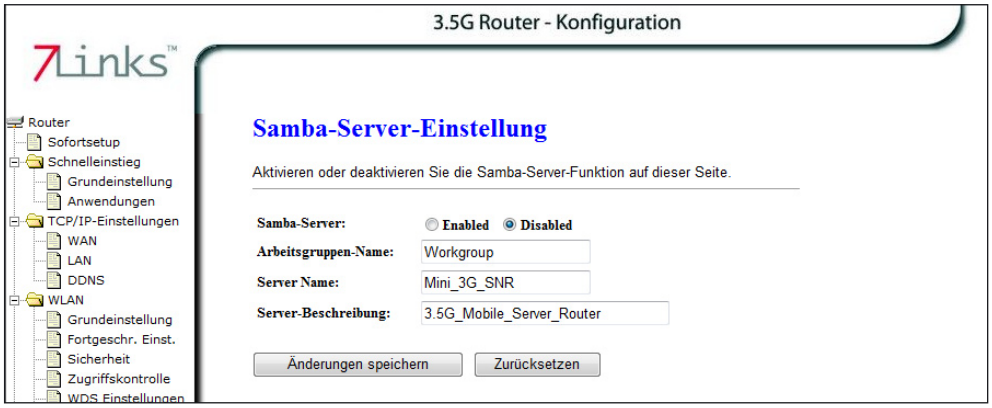
Option	Werte	Funktion
URL-Filter verwenden	Ein Aus	Filter aktivieren.
URL-Adresse	<text>	Diese URL sperren.

Beispiel



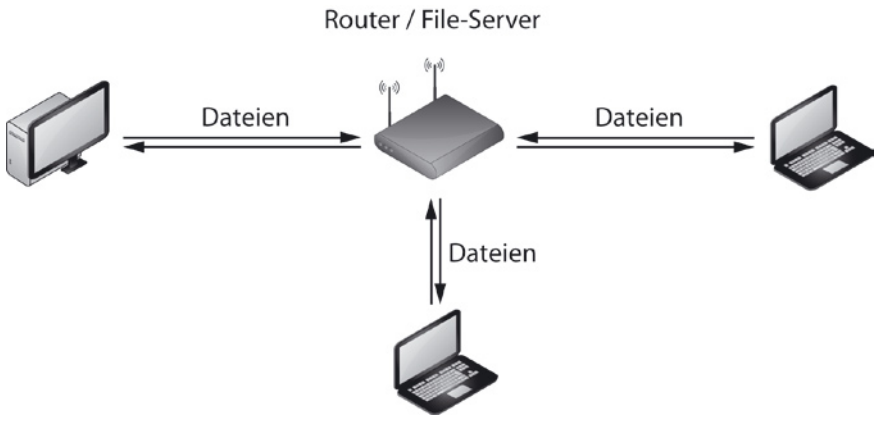
SERVER

Samba-Server

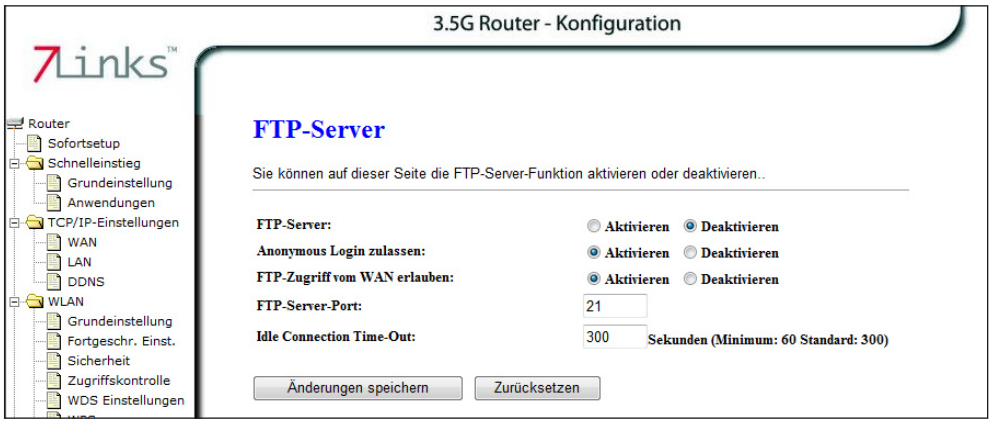


Option	Werte	Funktion
Samba-Server	Enabled Disabled	Samba-Server (Windows Netzwerkfreigabe) aktivieren oder deaktivieren.
Arbeitsgruppen-Name	<text>	Bezeichnung der Windows-Arbeitsgruppe.
Server Name	<text>	Bezeichnung der Freigabe.
Server Beschreibung	<text>	Beschreibung für die Freigabe.

Beispiel

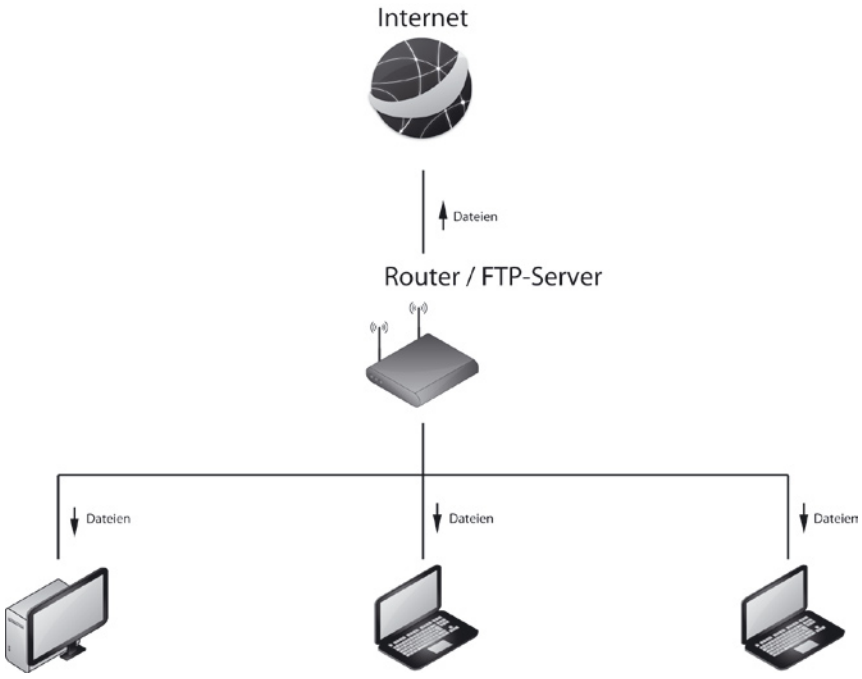


FTP-Server

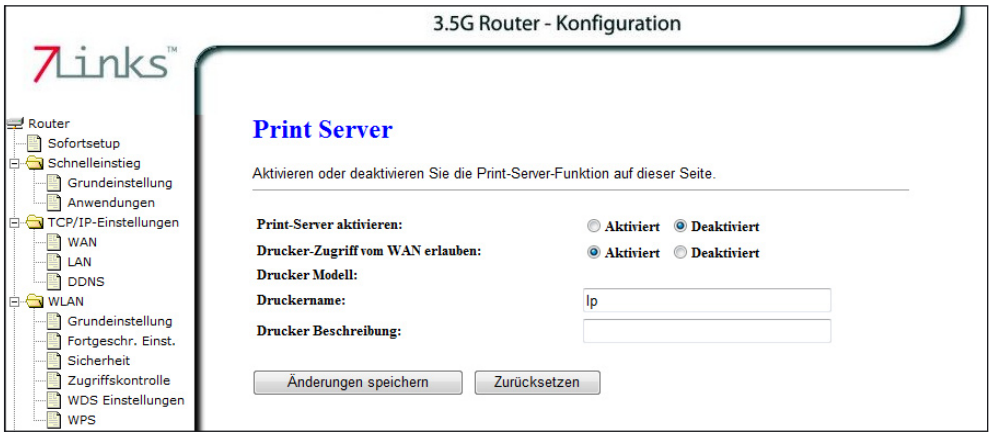


Option	Werte	Funktion
FTP-Server	Aktiviert Deaktiviert	FTP-Server aktivieren oder deaktivieren.
Anonymous Login zulassen	Aktiviert Deaktiviert	Erlaubt den Zugriff auf den FTP ohne Benutzeranmeldung.
FTP-Zugriff vom WAN erlauben	Aktiviert Deaktiviert	Erlaubt den Zugriff auf den FTP-Server über das Internet.
FTP-Server-Port	<text>	Port, der für den FTP-Server verwendet werden soll.
Idle Connection Time-Out	<text>	Zeit nach der inaktive Clients vom Server getrennt werden.

Beispiel



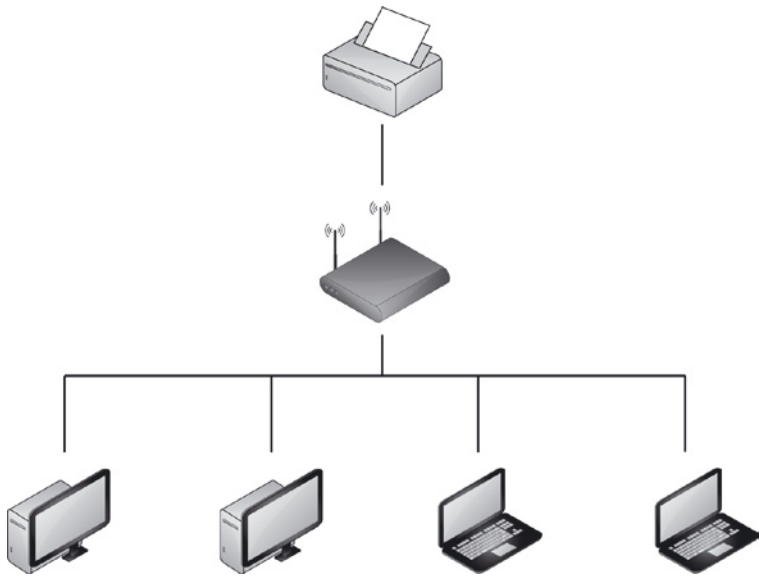
Print-Server



Option	Werte	Funktion
Print-Server aktivieren	Aktiviert Deaktiviert	Print-Server aktivieren oder deaktivieren.
Drucker-Zugriff vom WAN erlauben	Aktiviert Deaktiviert	Erlaubt den Zugriff auf den Drucker über das Internet.
Druckername	<text>	Bezeichnung des Druckers bei Zugriff über das Netzwerk.
Drucker Beschreibung	<text>	Kommentar.

Beispiel

HINWEIS:
Auch wenn Sie über das Netzwerk auf den Drucker zugreifen wollen, müssen die entsprechenden Treiber auf dem Computer installiert sein, der den Druckauftrag sendet.



MANAGEMENT

Passwort ändern

Option	Werte	Funktion
Neues Passwort	<text>	Verwenden Sie unbedingt sichere Passwörter ↘. Siehe Hinweise S. 63.
Passwort bestätigen	<text>	Passwort nochmals wiederholen.

Firmware Update

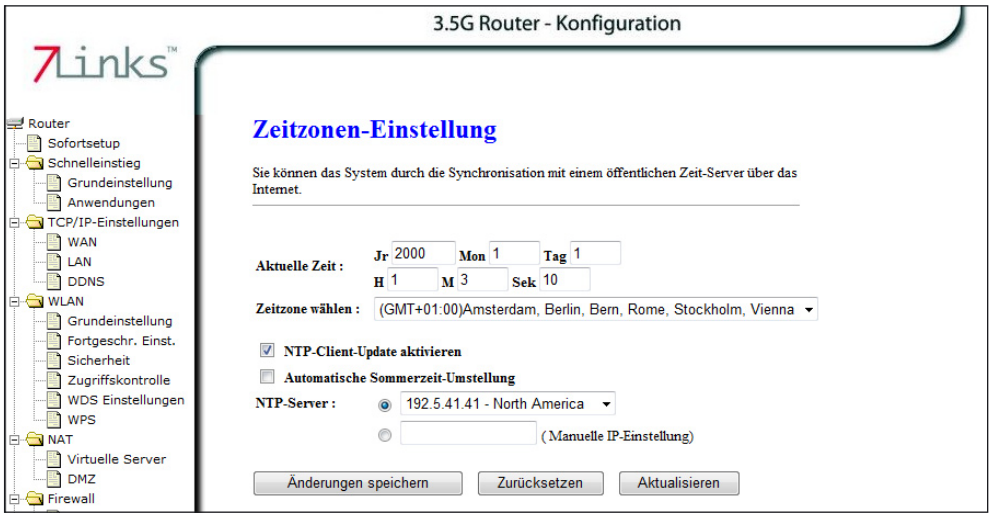
Wählen Sie eine lokale Datei, um ein Firmware-Update durchzuführen.
VERWENDEN SIE NUR VOM HERSTELLER AUTHORISIERTE UPDATES!

Profile speichern

Einstellungen in Datei speichern	<datei>	Speichert die Routereinstellungen in einer lokalen Datei.
Einstellungen aus Datei laden	<datei>	Lädt Routereinstellungen aus einer lokalen Datei.
Werkseinstellungen wieder herstellen		Router in den Auslieferungszustand zurücksetzen.

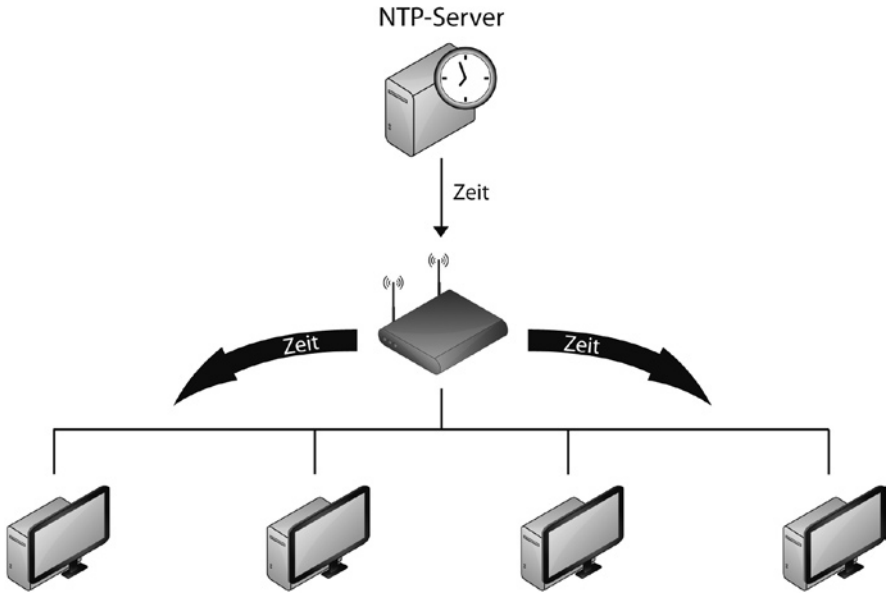
Dieser Menüpunkt erlaubt Ihnen die Nutzung mehrerer Einstellungsprofile, die Sie in lokalen Dateien speichern oder aus diesen wieder laden können. Dies empfiehlt sich immer dann, wenn Sie den Router in verschiedenen Netzwerken betreiben wollen.

NTP-Einstellungen



Option	Werte	Funktion
Aktuelle Zeit	<parameter>	Zeit für den Router einstellen.
Zeitzone wählen	<parameter>	Die Zeitzone einstellen in der der Router steht.
NTP-Client-Update aktivieren	Ein Aus	Zeitsynchronisation für Clients aktivieren.
Automatische Sommerzeit-Umstellung	Ein Aus	Automatisch auf Sommerzeit umstellen.
NTP Server	North America 1-3 Europa 1-2 Australia Asia Pacific Manuell	Externe Zeitserver zur Synchronisation.

Beispiel



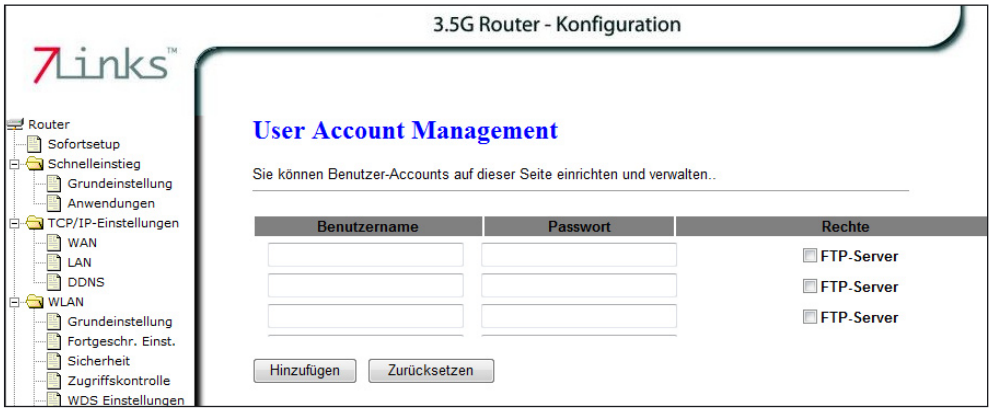
UPnP einstellen

Option	Werte	Funktion
uPNP verwenden	Ein Aus	uPNP-Verwendung erlauben.

Sprache ändern

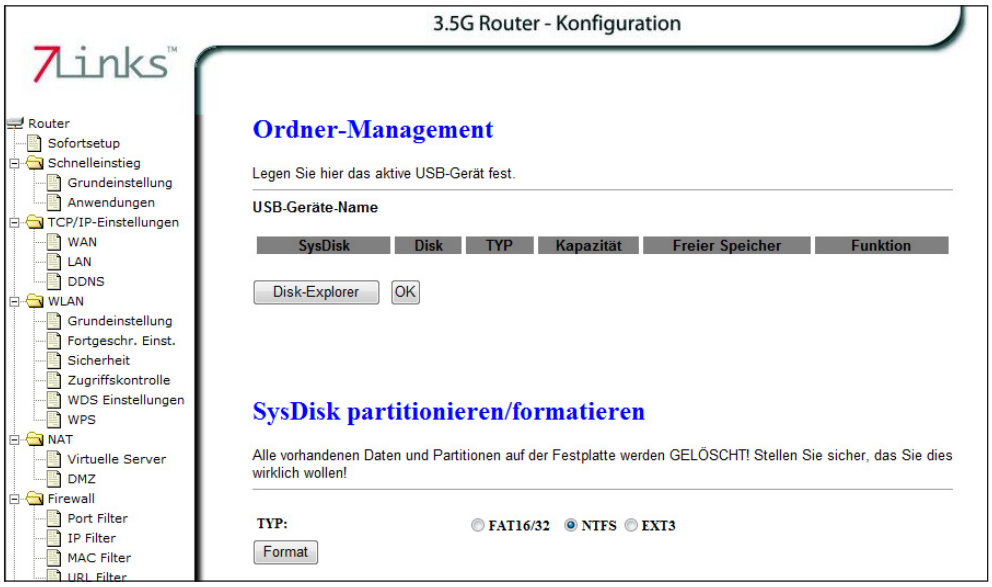
Einstellen der Verwendeten Sprache für die Routerkonfiguration.

User Accounts



Option	Werte	Funktion
Benutzername	<text>	Neuen Benutzernamen für den Zugriff auf die Serverdienste anlegen.
Passwort	<text>	Passwort für den Useraccount.
FTP-Server	Ein Aus	Zugriff auf den FTP-Server für diesen Nutzer zulassen.

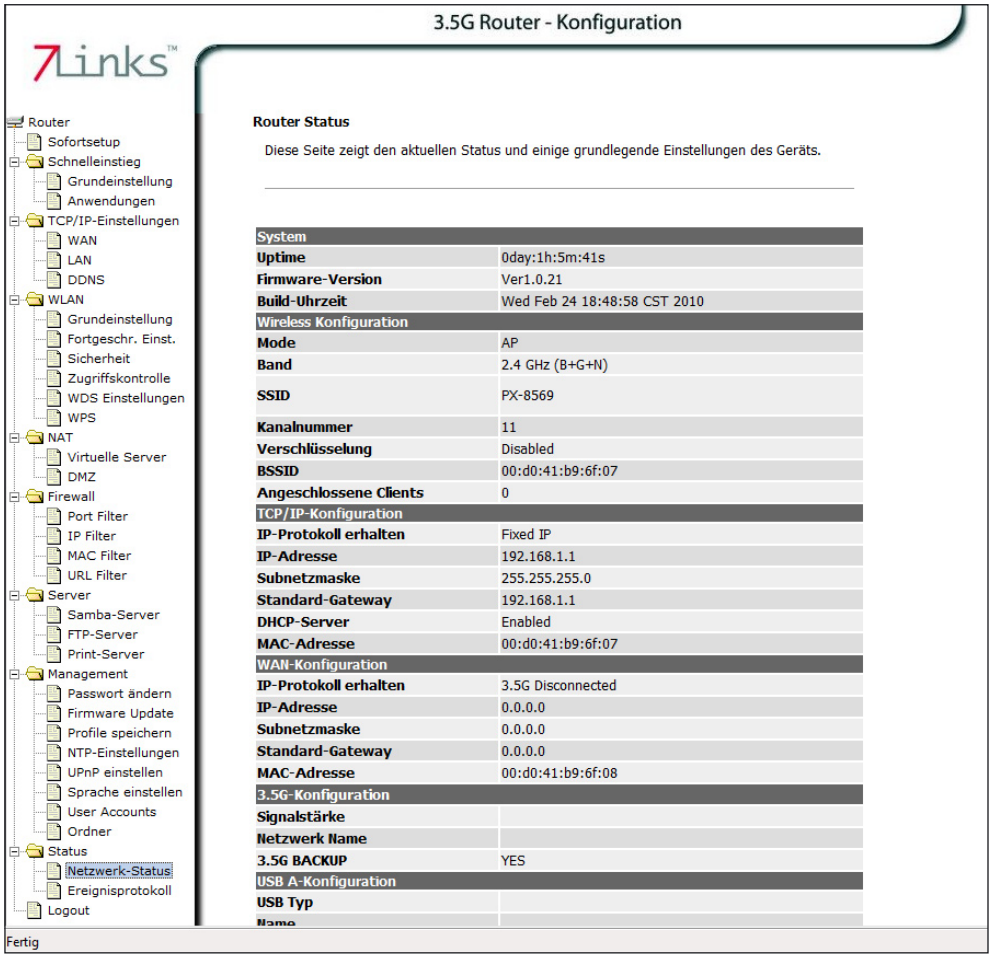
Ordner



Option	Werte	Funktion
Typ	FAT16/32 NTFS EXT3	Dateisystem mit dem der angeschlossene USB-Datenträger formatiert werden soll.

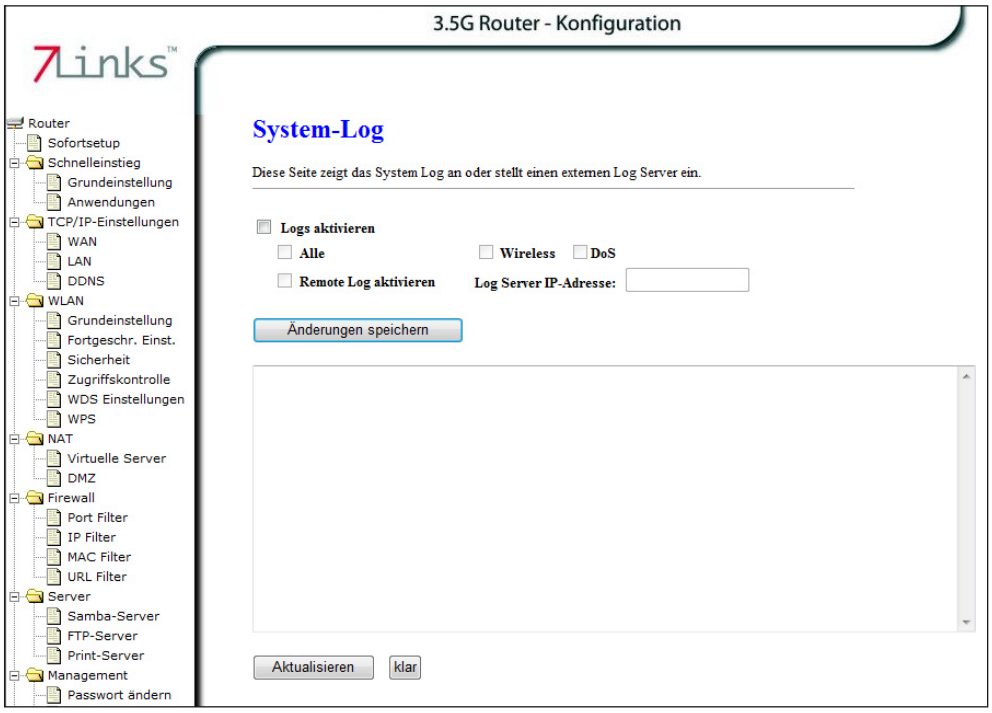
STATUS

Netzwerk-Status



Zeigt alle relevanten Konfigurations- und Verbindungsdaten des Routers an.

Ereignisprotokoll



Option	Werte	Funktion
Logs aktivieren	Ein Aus	Betriebslog für den Router erstellen.
Alle	Ein Aus	Alle Operationen des Routers aufzeichnen.
Wireless	Ein Aus	Die Wireless-Verbindungen aufzeichnen.
DoS	Ein Aus	DoS-Attacken aufzeichnen.
Remote Log aktivieren	Ein Aus	Logs auf einer externen Quelle ablegen.
Log Server IP-Adresse	<text>	IP-Adresse der externen Quelle.

ANHANG

BASISWISSEN NETZWERKE

Da bei Netzwerken häufig Unklarheiten und missverständliche Begriffe auftreten, soll dieses Glossar dabei helfen, Licht ins Dunkel mancher Fachbegriffe zu bringen. Im Folgenden werden die grundlegenden Hardwarekomponenten eines herkömmlichen Heimnetzwerks ebenso dargestellt, als auch die verwendeten Anwendungen und Dienste.

Hardware

- **Access-Point**
  Der Zugangspunkt oder auch Access-Point ist die „Basisstation" in einem drahtlosen Netzwerk (WLAN). Diese Funktion wird häufig in Heimnetzwerken auch von einem Router übernommen.

- **DSL-Modem**
  Das DSL-Modem verbindet Ihren Computer mit dem Internet. Wenn Sie mit mehr als einen Computer über eine Leitung Zugriff auf das Internet haben wollen, benötigen Sie einen Router, der direkt hinter das DSL-Modem geschaltet wird.

- **Kabelmodem**
  Als Kabelmodem bezeichnet man das Gerät, das Daten über Fernseh-Kabelnetze überträgt und für Breitband-Internetzugänge über Kabel-anschlüsse (Kabelinternet) eingesetzt wird.

- **Netzwerkhub**
  Netzwerkhubs wurden in der Vergangenheit als „Knotenpunkt" verwendet, um mehrere Netzwerkgeräte miteinander zu verbinden. Jedoch wurden Sie inzwischen weitestgehend durch Netzwerkswitches abgelöst.

- **Netzwerkkabel/Ethernetkabel**
  Hier gibt es zwei Varianten. So genannte „Patch"-Kabel und „Crossover"-Kabel.
  Patchkabel sind die Kabel, die am häufigsten Verwendung in Netz-werken finden. Sie werden eingesetzt, um Computer mit Switches, Hubs oder Routern zu verbinden.
  Crossover-Kabel werden dazu eingesetzt, um zwei Computer direkt miteinander zu verbinden, ohne ein Netzwerk zu verwenden.
  Patchkabel sind der gängige Lieferumfang von Netzwerkprodukten.

- **Netzwerkkarten**
  Netzwerkkarten werden in der heutigen Zeit oftmals schon auf den Hauptplatinen (Mainboards) integriert. Die Anschlüsse ähneln denen von Telefonanschlüssen.
  Der Stecker hierzu hat die technische Bezeichnung RJ-45. Sie dienen zur Datenübertragung an ein Netzwerk.

- **Netzwerkswitch**
  Switches werden als „Knotenpunkt“ von Netzwerken eingesetzt. Sie dienen dazu, mehrere Netzwerkgeräte „auf ein Kabel“ im Netzwerk zusammenzuführen. Switches sind häufig zu logischen Verbünden zusammengestellt und verbinden z.B. alle Computer aus einem Büro. Koppelt man mehrere Switches, erhält man ein komplexeres Netzwerk, welches einer Baumstruktur ähnelt.

- **Router**
  Router dienen zur Zugriffssteuerung von Netzwerkcomputern untereinander und regeln ebenfalls den Zugriff auf das Internet für alle sich im Netzwerk befindlichen Computer. Router werden sowohl rein kabelgebunden, als auch als WLAN-fähige Variante vertrieben. Meist übernehmen handelsübliche Router noch Sonderfunktionen wie z.B. DHCP, QoS, Firewall, NTP,…

- **WLAN-Karten und WLAN-Dongles**
  Zunehmend werden drahtlose Netzwerke eingesetzt, so genannte WLANs. Um eine Verbindung zu einem WLAN herstellen zu können, wird eine spezielle Hardware benötigt. Diese Hardware existiert häufig in Form von WLAN-Karten oder WLAN Dongles (-Sticks). WLAN-Karten werden in Desktop-Computern („normaler“ Computer) verwendet, während WLAN-Dongles häufig für den mobilen Einsatz gedacht sind (Notebooks) und werden über USB betrieben.

Grundlegende Netzwerkbegriffe

- **Adressbereich**
  Ein Adressbereich ist eine festgelegte Gruppe von IP- oder MAC- Adressen und fasst diese zu einer „Verwaltungseinheit“ zusammen.

- **Blacklist**
  Mit einer Blacklist bezeichnet man bei Netzwerken eine Liste von Geräten denen die Verbindung zu einem Gerät (z.B. Router) explizit nicht erlaubt ist. Alle anderen Geräte werden von dem Gerät akzeptiert, das den Zugang über die Blacklist regelt. Im Gegensatz dazu steht die so genannte Whitelist.

- **Browser**
  Browser werden Programme genannt die hauptsächlich zur Darstellung von Webseiten genutzt werden. Die bekanntesten Browser sind der Internet Explorer, Mozilla Firefox, Opera oder Google Chrome.

- **Client**
  Als Client wird jede Anwendung bezeichnet, die Daten eines Serverdienstes in Anspruch nimmt. Eine klassische Client-Server Bindung entsteht in Heimnetzwerken häufig schon bei der Vergabe von IP-Adressen im Netzwerk. Hier fordert der Computer als DHCP-Client eine gültige IP-Adresse vom DHCP-Server (meist der Router) an und erhält diese vom DHCP-Server zugeteilt.

- **OSI-Schichtenmodell (Aufbau von Netzwerken)**
  Das OSI-Schichtenmodell dient zur Veranschaulichung der in Netzwerken verwendeten Protokolle. Jede Ebene dieser Modelle baut auf die darunter liegenden Ebenen auf. So ist z.B. einem Gerät eine MAC-Adresse zugeordnet aber keine IP-Adresse (bei Switches); jedoch ist einem Gerät mit einer IP-Adresse IMMER auch eine MAC-Adresse zugeordnet.

- **IP-Adresse**
  IP-Adressen werden dazu verwendet Computer, Drucker oder andere Geräte flexibel in ein Netzwerk einzubinden. Hierbei ist zwischen globalen und privaten IP-Adressen zu unterscheiden. Globale IP-Adressen werden von den einzelnen Internet-Anbietern oftmals dynamisch (DHCP) vergeben. Sie dienen dazu, Ihr Heimnetzwerk oder auch nur den einzelnen Computer gegenüber dem Internet erreichbar zu machen. Private IP-Adressen werden im Heimnetzwerk entweder statisch („von Hand“ zugewiesen) oder dynamisch (DHCP) vom Anwender selbst vergeben. IP-Adressen ordnen ein spezielles Gerät eindeutig einem bestimmten Netzwerk zu.

BEISPIEL:
IP-Adressen sind die bekanntesten Adressierungen im Netzwerk und treten in folgender Form auf: z.B. 192.168.0.1

- **ISP**
  ISP ist die Abkürzung für „Internet Service Provider“. Dieser Begriff wird für Stellen verwendet, die einem Netzwerk oder Einzelcomputer den Zugang zum Internet anbieten. In Deutschland ist der wohl bekannteste ISP T-Online, aber auch Anbieter wie Freenet, Arcor, 1&1 oder KabelDeutschland gehören zu den ISPs.

- **LAN**
  LAN (Local Area Network) bezeichnet ein Netzwerk aus Computern und anderen Netzwerkgeräten, die über einen gemeinsamen Adressbereich verfügen und damit zu einer Struktur zusammengefasst werden.

- **MAC-Adresse**
  Als MAC-Adresse bezeichnet man die physikalische Adresse einer Netzwerkkomponente (z.B. Netzwerkkarte, WLAN-Dongle, Drucker, Switch). MAC-Adressen sind entgegen IP-Adressen immer eindeutig zuordenbar.
  MAC-Adressen von anderen verbundenen Netzwerkgeräten werden von den einzelnen Geräten jeweils in einer so genannten ARP-Tabelle gespeichert. Diese ARP-Tabellen können zur Fehlersuche dienen, falls ein Gerät ohne IP-Adresse (z.B. Switch) im Netzwerk keine Funktion zeigt.

  BEISPIEL:
  Eine MAC-Adresse sieht z.B. so aus: 00:00:C0:5A:42:C1

- **Passphrase**
  Mit dem Begriff Passphrase wird ein Schlüsselwort oder Satz umschrieben, der als Sicherheitsabfrage bei der Verbindung zu WPA-/WPA2-Verschlüsselten Netzwerken eingegeben werden muss.

- **Port**
  Als Port wird eine Softwareschnittstelle bezeichnet, die es einzelnen Anwendungen auf Ihrem Computer ermöglicht, mit den Anwendungen eines Anbieters zu kommunizieren. Hier wird hauptsächlich zwischen zwei Protokollen unterschieden: TCP und UDP.

  BEISPIEL:
  Die häufigste Internet-Anwendung ist ein Browser (Internet Explorer, Mozilla Firefox, usw.), welcher meist über den TCP-Port 80 mit den Servern der Webseiten-Anbieter kommuniziert.

- **POE**
  Power over Ethernet (PoE) bezeichnet ein Verfahren, mit dem netzwerkfähige Geräte über das Ethernet-Kabel mit Strom versorgt werden können.

- **Protokoll**
  Protokolle im Netzwerk sind Standards für Datenpakete, die Netzwerkgeräte untereinander austauschen, um eine eindeutige Kommunikation zu ermöglichen.

- **Pre-Shared Key**
  Mit Pre-Shared Key („vorher vereinbarter Schlüssel“) oder kurz PSK bezeichnet man ein Verschlüsselungsverfahren, bei denen die verwendeten Schlüssel vor der Verbindung beiden Teilnehmern bekannt sein muss (siehe auch WPA/WPA2).

- **Sichere Passwörter**
  Unter sicheren Passwörtern versteht man Passwörter, die bestimmte Bedingungen erfüllen, um von Angreifern nicht mit einfachsten Mitteln entschlüsselt werden zu können.
  Sichere Passwörter sollten generell eine bestimmte Mindestlänge aufweisen und mehrere Sonderzeichen beinhalten. Als Faustregel gilt hier: Je länger das Passwort ist und je mehr Sonderzeichen es beinhaltet, desto sicherer ist es gegen Entschlüsselung.

- **SSID**
  SSID (Service Set Identifier) steht für die Bezeichnung, die für ein WLAN-Netzwerk verwendet wird. Diese SSID wird meist per Broadcast (siehe UDP) öffentlich ausgesendet, um das Netzwerk für mobile Geräte „sichtbar“ zu machen.

- **Subnetz**
  Subnetze sind eine Zusammenfassung von einzelnen IP-Adressen zu Netzwerkstrukturen. So werden meist Computer einer Abteilung im Büro in einem Subnetz zusammengefasst, während die Computer einer anderen Abteilung in einem weiteren Subnetz zusammengefasst sind. Daher sind Subnetze eine reine Strukturierungsmaßnahme. Eine Angabe des Subnetzraumes wird immer in Zusammenhang mit der Vergabe einer IP-Adresse durchgeführt. Im Heimbereich werden normalerweise keine speziellen Subnetze eingerichtet. Daher ist bei Windows-Systemen als Subnetzmaske die 255.255.255.0 voreingestellt. Dadurch stehen die IP-Adressen xxx.xxx.xxx.1 bis xxx.xxx.xxx.254 zur Verfügung.

- **TCP (Transmission Control Protocol)**
  Das TCP-Protokoll wird dazu verwendet, gezielt Informationen von einem speziellen Gegenüber abzufragen (siehe Beispiel bei Port)

- **Traffic**
  Mit Traffic bezeichnet man die ausgetauschten Datenmengen zwischen zwei Stellen oder aber auch den gesamten Datenverkehr in einem Netzwerkabschnitt.

- **UDP (User Datagram Protocol)**
  Das UDP-Protokoll ist ein so genanntes „Broadcast“-Protokoll. Broadcast wird im englischen auch für Radio- oder TV-Sendungen verwendet. Ganz ähnlich arbeitet dieses Protokoll. Es wird verwendet, um Datenpakete an alle im Netzwerk erreichbaren Geräte zu senden und im Weiteren auf Rückmeldung dieser Geräte zu warten. Das UDP-Protokoll wird meist dann von Anwendungen eingesetzt, wenn unsicher ist ob eine entsprechende Gegenstelle im Netzwerk vorhanden ist.

- **uPNP**
  Mit diesem Begriff wird das „universal Plug and Play"-Protokoll bezeichnet. Dieses Protokoll wird hauptsächlich dazu verwendet, Drucker und ähnliche Peripheriegeräte über ein Netzwerk ansteuern zu können.

- **Verschlüsselung**
  Verschlüsselungsmechanismen werden in Netzwerken dazu eingesetzt, Ihre Daten vor fremdem Zugriff abzusichern. Diese Verschlüsselungsme-chanismen funktionieren ähnlich wie bei einer EC-Karte. Nur mit dem richtigen Passwort (der richtigen PIN) können die Daten entschlüsselt werden.

- **VPN**
  VPN (Virtual Private Network) steht für eine Schnittstelle in einem Netzwerk, die es ermöglicht, Geräte an ein benachbartes Netz zu binden, ohne dass die Netzwerke miteinander kompatibel sein müssen.

- **WAN**
  WAN (Wide Area Network) bezeichnet ein Netzwerk aus Computern und anderen Netzwerkgeräten, die über größere Entfernungen und aus vielen Bestandteilen zusammengefasst werden. Das bekannteste Beispiel ist das „Internet". Jedoch kann ein WAN auch nur aus zwei räumlich voneinander getrennten LANs bestehen.

- **Whitelist**
  Mit einer Whitelist bezeichnet man bei Netzwerken eine Liste von Geräten denen die Verbindung zu einem Gerät (z.B. Router) explizit erlaubt ist. Alle anderen Geräte werden von dem Gerät abgewiesen, das den Zugang über die Whitelist regelt. Im Gegensatz dazu steht die so genannte Blacklist.

Dienste in Netzwerken

- **DHCP (Dynamic Host Configuration Protocol)**
  Mit DHCP wird die dynamische Verteilung von IP-Adressen in Netzwerken bezeichnet. Dynamisch sind diese Adressen deshalb, weil Sie jederzeit ohne größeren Aufwand neu vergeben werden können. Man kann dynamische IP-Adressen auch als geliehene IP-Adressen bezeichnen.
  Diese geliehenen IP-Adressen werden mit einem „Verfallsdatum" versehen – der so genannten „Lease Time". Ein Computer wird am DHCP-Server nur dann nach einer neuen IP-Adresse anfragen, wenn sein „Lease" abgelaufen ist. Dies ist allerdings auch eine mögliche Fehlerquelle, da es hier zu Unstimmigkeiten zwischen DHCP-Server und DHCP-Clients kommen kann.

  HINWEIS:
  Windows Computer sind standardmäßig als DHCP-Client eingestellt, um einen einfachen Anschluss an ein Heimnetzwerk zu ermöglichen.

- **DNS (Domain Name Server)**
  DNS ist ein Serverdienst, der die Übersetzung von IP-Adressen in gängige Internet-Adressen übernimmt. So wird z.B. aus
  www.google.de die IP-Adresse: 74.125.39.105. Werden Sie während einer Konfiguration aufgefordert, die DNS-IP-Adresse einzugeben, ist damit immer die Adresse desjenigen Servers gesucht, welcher den DNS-Serverdienst anbietet. DNS-Server werden aus Gründen der Ausfallsicherheit meist doppelt angegeben und als Primärer DNS (oder DNS1), bzw. Sekundärer DNS (oder DNS2) bezeichnet.

- **Filter** und **Firewall**
  Eine Firewall ist ein Sicherungsmechanismus, welcher meist auf Routern als Serverdienst läuft, jedoch bereits in Windows (seit XP) integriert ist. Sie erlaubt nur Zugriffe auf voreingestellte Ports, blockt vorher konfigurierte IP-Adressen und soll generell schädliche Angriffe auf Ihr Netzwerk verhindern.

- **FTP/NAS (File Transfer Protocol/ Network Access Storage)**
  FTP ist ein Serverdienst, der hauptsächlich zum Transfer von Dateien verwendet wird. Dieser Dienst ermöglicht es auf unkomplizierte Art und Weise Dateien von einem Computer auf einen entfernt stehenden anderen Computer ähnlich dem Windows Explorer zu übertragen. So genannte NAS-Server setzen ebenfalls häufig diesen Dienst ein, um einen Zugriff aus dem gesamten Netzwerk auf eine Festplatte zu erlauben.

- **(Standard-) Gateway**
  Als Gateway wird die Schnittstelle bezeichnet, die es den Computern im privaten Netzwerk ermöglicht, mit Computern außerhalb zu kommunizieren. Es ist in diesem Sinne mit Ihrem Router gleichzusetzen. Das Gateway sammelt und sendet Anfragen der Clients und leitet diese weiter an die entsprechenden Server im Internet. Ebenso verteilt das Gateway die Antworten der Server wieder an die Clients, die die Anfrage gestellt hatten.

- **HTTP/Webserver (Hypertext Transfer Protocol)**
  Dieser Dienst ist das, was in der Öffentlichkeit als „Das Internet“ bezeichnet wird. Jedoch handelt es sich hier bei nur um eine Vereinfachung, da das Internet an sich eine übergeordnete Struktur ist, welche nahezu alle Serverdienste beinhaltet. HTTP wird zum Transfer und der Darstellung von Webseiten verwendet.

- **Mediastreams**
  Diese Gruppe von Serverdiensten wird von vielfältigen Geräten und Anbietern verwendet. Die bekanntesten Beispiele sind Internet-Radiosender, Video-On-Demand und IP-Kameras. Diese Streams nutzen teils unterschiedliche Protokolle und Protokollversionen. Daher kann es hier durchaus einmal zu Inkompatibilitäten zwischen Server und Client kommen.

- **NTP**
  NTP (Network Time Protcol) bezeichnet ein Protokoll, mit dem Computer über das Netzwerk Ihre Datums- und Zeiteinstellungen abgleichen können. Dieser Dienst wird von weltweit verteilten Servern bereitgestellt.

- **PPPoE**
  PPPoE steht für PPP over Ethernet und bezeichnet Verwendung des Netzwerkprotokolls Point-to-Point Protocol (PPP) über eine Ethernet-Verbindung. PPPoE wird in Deutschland hauptsächlich in Verbindung mit ADSL-Anschlüssen verwendet. ADSL bedeutet Asynchrones DSL und steht für die Verwendung einer Leitung für Telefon und Internet. ADSL ist Standard in Deutschland.
  Hauptgrund für die Verwendung von PPPoE ist die Möglichkeit, Authentifizierung und Netzwerkkonfiguration (IP-Adresse, Gateway) auf dem schnelleren Ethernet zur Verfügung zu stellen.

- **PPTP**
  Protokoll zum Aufbau einer VPN-Netzwerkverbindung (Point-to-Point-Transfer-Protokoll).

- **QoS (Quality of Service)**
  QoS wird in Netzwerken dazu verwendet, für bestimmte Clients oder Dienste eine bestimmte, garantierte Bandbreite für den Datenverkehr zu gewährleisten. Als Vergleich lässt sich eine Autobahn heranziehen, auf der selbst bei einem Stau die Standspur von Rettungsfahrzeugen genutzt werden kann, um voranzukommen. QoS wird also immer dann verwendet, wenn sichergestellt werden soll, dass bestimmte Dienste immer verfügbar sein sollen – ohne dabei auf den restlichen Datenverkehr Rücksicht nehmen zu müssen.

- **Samba/SMB**
  Mit diesen Begriffen ist ein Serverdienst gemeint, der speziell in Windows Netzwerken verwendet wird. Dieser Service ermöglicht ebenfalls den schnellen und einfachen Zugriff auf Dateien die sich auf anderen Computern befinden (in so genannten „freigegebenen Ordnern“). Jedoch ist dieser Dienst auf Heimnetzwerke begrenzt und kann nur in Ausnahmefällen auch über das Internet in Anspruch genommen werden.

- **Server/Serverdienst**
  Ein Server ist immer als Anbieter von Netzwerkdiensten zu sehen. Einzelne Anwendungen werden auch als Serverdienst bezeichnet. Die bekanntesten Serverdienste sind unter anderem Webserver, DHCP oder E-Mail Server. Mehrere solche Dienste können auf einem Computer oder anderen Geräten (z.B. Routern) gleichzeitig verfügbar sein. Server werden auch Computer genannt, deren ausschließliche Funktion darin besteht, Serverdienste anzubieten und zu verwalten.

- **Statische Adressvergabe**
  Bei der statischen Adressvergabe sind alle Netzwerkadressen eines Netzwerkes fest vergeben. Jeder einzelne Client (Computer) des Netz-werks hat seine feste IP-Adresse, die Subnetzmaske, das Standard-Gateway und den DNS-Server fest eingespeichert und muss sich mit diesen Daten beim Server anmelden. Ein neuer Client (Computer) muss erst mit einer gültigen, noch nicht vergebenen IP-Adresse und den restlichen Daten ausgestattet werden, bevor er das Netzwerk nutzen kann. Manuelle Adressvergabe ist besonders bei Netzwerkdruckern oder ähnlichen Geräten sinnvoll, auf die häufig zugegriffen werden muss oder in Netzwerken, die besonders sicher sein müssen.

- **Torrents**
  Auch bei Torrents handelt es sich um einen Datei-Transfer-Dienst. Diesen Dienst kann man in gewisser Weise als „verteiltes FTP“ ansehen, da hier der Datentransfer von einzelnen Dateien von mehreren Anbietern („Seeds“) angefordert wird. Dazu müssen die Dateien nicht einmal vollständig beim Anbieter vorhanden sein (diese laden die gleiche Datei ebenfalls herunter – bieten aber schon vorhandene Dateiteile ebenfalls an). Diese „unfertigen“ Quellen werden als „Leeches“ bezeichnet.

- **WEP und WPA**
  Wired Equivalent Privacy (WEP) ist der ehemalige Standard-Verschlüs-selungsalgorithmus für WLAN. Er soll sowohl den Zugang zum Netz regeln, als auch die Vertraulichkeit der Daten sicherstellen. Aufgrund verschiedener Schwachstellen wird das Verfahren als unsicher angesehen. Daher sollten WLAN-Installationen die sicherere WPA-Verschlüsselung verwenden.
  Wi-Fi Protected Access (WPA) ist eine modernere Verschlüsselungsmethode für ein WLAN. Sie wurde als Nachfolger von WEP eingeführt und weist nicht deren Schwachstellen auf.

SICHERHEITSMASSNAHMEN IN WLAN-NETZWERKEN

An erster Stelle sollten der Verzicht von WEP und der Einsatz von WPA oder WPA2 stehen. Dieses Ziel lässt sich in vielen Fällen bereits durch ein Treiber- oder Firmwareupdate erreichen. Lässt sich der Einsatz von WEP nicht vermeiden, sollten folgende grundlegende Behelfsmaßnahmen beachtet werden, um das Risiko von Angriffen fremder Personen auf das WLAN zu minimieren:

- Aktivieren Sie auf alle Fälle den Passwortschutz! Ändern Sie ggf. das Standard-Passwort des Access Points.
- Wenn Sie die WEP-Verschlüsselung verwenden, weil eines der angeschlossenen Geräte WPA oder WPA2 (dringend empfohlen) nicht unterstützt wird, sollte der WEP-Schlüssel mindestens 128 Bit lang sein und eine lose Kombination aus Buchstaben, Ziffern und Sonderzeichen darstellen.
- Aktivieren Sie die Zugriffskontrollliste (ACL = Access Control List), um vom Access Point nur Endgeräte mit bekannter MAC-Adresse zuzulassen. Beachten Sie, dass sich eine MAC-Adresse aber mittels Treiber beliebig einstellen lässt, sodass eine mitgelesene zugelassene MAC-Adresse leicht als eigene ausgegeben werden kann.
- Verwenden Sie eine sinnvolle SSID: Die SSID des Access Point sollte keine Rückschlüsse auf Ihren Namen, verwendete Hardware, Einsatzzweck und Einsatzort zulassen.
- Umstritten ist die Deaktivierung der SSID-Übermittlung (Broadcasting). Sie verhindert das unabsichtliche Einbuchen in das WLAN, jedoch kann die SSID bei deaktiviertem Broadcasting mit einem so genannten Sniffer (Gerät zur LAN-Analyse) mitgelesen werden, wenn sich etwa ein Endgerät beim Access Point anmeldet.
- WLAN-Geräte (wie der Access Point) sollten nicht per WLAN konfiguriert werden, sondern ausschließlich über eine kabelgebundene Verbindung.
- Schalten Sie WLAN-Geräte stets aus, wenn Sie sie nicht benutzen.
- Führen Sie regelmäßige Firmware-Updates vom Access Point durch, um sicherheitsrelevante Aktualisierungen zu erhalten.
- Reichweite des WLANs durch Reduzierung der Sendeleistung bzw. Standortwahl des WLAN Gerätes beeinflussen (Dies dient allerdings nicht der aktiven Sicherheit, sondern begrenzt lediglich den möglichen Angriffsbereich.)

Alle diese Sicherheitsmaßnahmen dürfen aber nicht darüber hinwegtäuschen, dass diese letztlich keinen wirklichen Schutz beim Einsatz von WEP bedeuten. Ein erfolgreicher Angriff auf die WEP-Verschlüsselung ist trotz all dieser Vorkehrungen mit den richtigen technischen Voraussetzungen innerhalb von 5 bis 10 Minuten mit ziemlicher Sicherheit erfolgreich.

INFORMATIONEN ZUR ENTSORGUNG VON ELEKTRONISCHEN GERÄTEN

Ihr neues Produkt wurde mit größter Sorgfalt entwickelt und aus hochwertigen Komponenten gefertigt. Trotzdem muss das Produkt eines Tages entsorgt werden. Die durchgestrichene Mülltonne bedeutet, dass Ihr Produkt am Ende seiner Lebensdauer getrennt vom Hausmüll entsorgt werden muss. Bitte bringen Sie in Zukunft alle elektrischen oder elektronischen Geräte zu den eingerichteten kommunalen Sammelstellen in Ihrer Gemeinde. Diese nehmen Ihre Geräte entgegen und sorgen für eine ordnungsgemäße und umweltgerechte Verarbeitung. Dadurch verhindern Sie mögliche schädliche Auswirkungen auf Mensch und Umwelt, die sich durch unsachgemäße Handhabung von Produkten am Ende von deren Lebensdauer ergeben können. Genaue Informationen zur nächstgelegenen Sammelstelle erhalten Sie bei Ihrer Gemeinde.

TECHNISCHE DATEN

Antenne	2 dBi bei 2,45GHz
Standard	IEEE 802.11g/b/n
Frequenzband	2,400GHz bis 2,450GHz
Service	FTP, WINS, Printserver, DHCP, DNS, DDNS, WDS, WPS
WAN Protokolle	PPPoE / PPTP / Statische IP/ Dynamische IP/ HSDPA/UMTS
Arbeitstemperatur	0°C bis 40°C
Betriebsluftfeuchtigkeit	10% ~ 90% (nicht kondensierend)
Anschlüsse	1 x RJ-45 Port für WAN/LAN 10/100 MBit 1 x RJ-45 Port LAN 10/100 MBit 2 x USB 2.0
Stromversorgung	12 V / 2,5 A
Sicherheit	64/128bit WEP WPA(TKIP mit IEEE 802.1x) WPA2(AES mit IEEE 802.1x)
Empfindlichkeit	11 Mbps: 10-5 BER @ -83 dBm
Maße (mm)	91 mm (L) x 80 mm (B) x 29 mm (H)
Gewicht	ca. 210 g

KONFORMITÄTSERKLÄRUNG

Hiermit erklärt Pearl Agency, dass sich dieses Produkt PX-8569-675 in Übereinstimmung mit den grundlegenden Anforderungen der Richtlinie 1999/5/EG befindet.

Pearl Agency
Pearl-Str. 1-3
79426 Buggingen
Deutschland
10.3.2010

Die ausführliche Konformitätserklärung finden Sie unter www.pearl.de.

CHECKLISTE FÜR DIE KONFIGURATION

Aufgabe	Erledigt
Funkkameraüberwachung ausschalten	
Schnurlostelefon ausschalten	
Sonstige Geräte mit 2,4 GHz ausschalten	
Stromversorgung mit Überspannungsschutz sichern	
Firewall am Computer ausstellen	
Firewall am vorhandenen Router ausstellen	
Virenscanner am Computer ausschalten	
MAC-Adressenfilter am vorhandenen Router ausschalten	
Verschlüsselung im Netzwerk ausschalten	
Benötigte Protokolle notieren	

Notwendige Daten	Kommentar
Netzwerk SSID	
IP – Gateway	
IP – DNS-Server	
DHCP Range	
Subnetzmaske	
IP – Internetzugang	
IP – Timeserver	
Passwort – Internetzugang	
Passwort – WLAN	
IPs von vorhandenen Servern	
IP – Log-Server	
IP – virtuelle DMZ	
Benötigte Protokolle	

© 03/2010 - LG//AK//BR - GS